Research Article

Performances evaluation of threshold-based IDS and trust based IDS under smart black hole attacks

Dr. Kheireddine MEKKAOUI[a] and Ishak MEDDAH[b]

[a] Department of computer sciences, University of Saida - Dr Moulay Tahar, Algeria, kheireddine.mekkaoui@univ-saida.dz
[b] Department of computer sciences, University of Saida - Dr Moulay Tahar, Algeria, ishak.meddah@univ-saida.dz

Article History: Received: 15 September 2022, Accepted: 06 December 2022, Available online 12 January 2023

Abstract: MANETs are ad Hoc networks characterized by dynamic topologies over time, open wireless medium, infrastructure less to control communications... etc. These networks are susceptible to various denial of service attacks such as black holes, which are considered among the most dangerous and serious threats. In order to mitigate black hole attacks, several intrusion detection systems have been proposed, like sequence number-based systems and trust-based systems, unfortunately these systems has become inefficient against the new wave of black holes, known also by smart black holes. Indeed, for example smart black holes can defeat threshold-based systems, by predicting the fixed threshold of the sequence number and can defeat the trust-based systems by checking if the RREQ is valid or not. In this paper, we have studied the impact of smart black holes on sequence number based systems and trust-based systems. We simulated, in NS2.35, several ad hoc networks with different densities under different number of smart black holes. Through simulation, it has been found that the smart black holes can easily defeat most of the proposed IDS in the literature.

Keywords: MANET, Smart black hole, AODV, intrusion detection system (IDS), Packet delivery ratio, Average throughput, Average End-to-End delay.

1.Introduction

Recent development in computer sciences, electronics and in telecommunication field allowed the appearance of small connected devices, equipped with limited batteries, small memories and low processors. These devices, called also nodes, can be either static or mobile. Actually, we are surrounded by several connected objects; we can find connected shoes, connected car, connected refrigerator ...etc. Indeed, according to **de Souza et al (2021)**, CISCO predicts that the number of connected objects will reach 500 billion in 2025.

These objects (or nodes), can operate in static or mobile environment in a completely decentralized manner, without the use of any base station **(Quy et al, 2021)**, forming, thus, a very promising type of networks, known by Mobile Ad hoc networks (MANETs).

A Mobile Ad hoc network (MANET) consists of several mobile nodes, forming dynamically a multi-hop wireless network, without any use of any infrastructure, these nodes are, often, deployed in a geographical zone for purposes of: control, monitoring or tracking **(Kariyannavar, S. S. et al, 2021)**.

In MANETs, communications are handled by routing protocols. These routing protocols are often classified into three principal categories: reactive, proactive and hybrid protocols **(Soomro, A. M. et al, 2022) (Thamizhmaran, K., & CHARLES, A., 2022)**. Reactive protocols, as AODV **(Perkins, C., et al, 2003)** and DSR (**Cheng, Y., et al, 2012),** are on demand protocols, routes established are only when needed by a source. Proactive protocol, as DSDV **(Arega, K. L. et al, 2020)** and WRP **(Rajeswari, A. R., 2020)**, are table driven protocols which stock all paths even when are not needed. Hybrid protocols, as ZPR (**Bhushan, B., & Sahoo, G., 2019)** and TORA **(AlKhatieb, A., et al, 2020)**, are a combination between reactive and proactive protocols.

In Mobile ad hoc networks, a node can be a source node, a destination node or a router **(Dhama, S. et al, 2016, Bolla et al 2023)**. Indeed, when the source and destination node are in range of each other, the communication between them is direct by using one hop communication. However, when the destination node is out of range of the source node, the multi hops communication is used, by implying the intermediate nodes, between them, to act as routers **(Al Rubaiei et al, 2022)**. Messages are forwarded to final destination using multi hops routing mechanism, where any node can freely participate in the ad hoc routing scheme, due to no administrator exists, which is considered as inherent problem to the network security, giving thus, the possibility to malicious nodes to join the routing multi hop paths, where the eavesdropping or data packet falsification may occur **(Arega, K. L., Raga, G., & Bareto, R., 2020)**.

Among several types of attack, black hole is one of the most serious threats in MANETs. In black hole attacks, an attacking node re-directs data packets to itself, by announcing itself the node having the newest and shortest path to the destination, then eavesdrops or discards the intercepted data, affecting, by this the network performances, hence the need to implement Intrusion Detection Systems (IDS) **(Mehdi, S. A., & Hussain, S. Z., 2023)**.

Intrusion detection system (IDS) refers to the analysis of events that occur in a network and checking whether if these events are normal or harmful **(Bhati, N. S. et al, 2020)**. These systems play an important role in network security, and it is considered as primary research area. Many IDS were proposed to deal with black hole attacks, but most of them became inefficient against the new generation of black holes, called also smart black holes. Indeed, classical solutions, like threshold-based IDS **(Tami A. et al, 2021); (Gurung, S., & Chauhan, S. ,2019); (Mehdi, S. A., & Hussain, S. Z., 2023); (Ram, A. et al, 2021)** which consists in fixing a threshold for the sequence number in order to detect the malicious node that assumes possessing a route to the destination with a very high sequence number, are invalid versus the smart black holes **(Terai, T., et al, 2020)**.

In this article, we are interested in evaluating the performance of the AODV protocol in MANET networks under several intelligent attacks, even in the case of the existence of IDS. The simulations made in network simulator NS2 showed that several proposed IDS have failed to stop smart black holes.

The rest of the paper is structured as follows: Section 2 describes AODV routing protocol, followed by a brief description of the Intrusion Detection Systems (IDS) in section 3. Related works are described in section 3. An overview of Smart black hole Attacks is presented in Section 4. Simulations and performances evaluation of the smart black hole attacks can be found in Section 6. Finally, section 7 contains the conclusion with perspectives.

2.AODV Routing Protocol

AODV is a reactive routing protocol widely used in MANETs **(Perkins, C., et al, 2003)**. A Route is established between two nodes (source and destination) on demand only when the source node has to share information with the destination, thus, no routes are saved beforehand. This protocol supports the mobility of nodes and it is characterised by **(Zaatouri, I., et al, 2019):**

- Reduced number of messages within the network in order to establish a route,
- Minimal control overhead,
- Minimal processing overhead,
- Multi-hop routing scheme,
- Dynamic topology maintenance,
- Loop-free routing process.

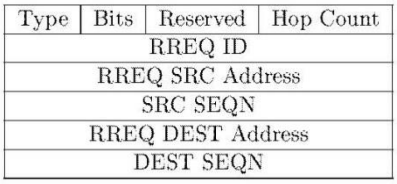
In AODV, route's procedure establishment is executed when the source node have to share information with the destination node, this procedure is based, principally, on the sequence number and the number of hop. Sequence number is used to determine if either the route is fresh or not and the number of hops is used to select the shortest path. During the establishment route process, four messages are exchanged **(Perkins, C., et al, 2003)**:

- Route request (RREQ),
- Route reply (RREP),
- Route error (RERR),
- Hello messages (Hello)

2.1.AODV Route construction

When a node wishes to establish a communication with a distant node, it checks first if it has a valid route to that destination, if not it initiate the route construction procedure, by broadcasting a RREQ Message, which is depicted in figure 1 **(Kumar, A. et al, 2023)**.

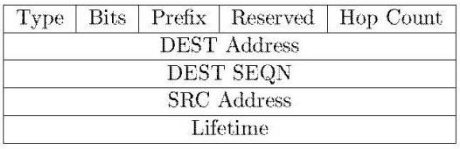
Figure.1.RREQ Message



Type	Bits	Reserved	Hop Count
RREQ ID			
RREQ SRC Address			
SRC SEQN			
RREQ DEST Address			
DEST SEQN			

When a neighbour node receives the RREQ, it checks for possible route to the destination in its routing table; if it has a valid route to the destination, it replies with a RREP, which is presented in figure 2, to the source node originator of RREQ; otherwise it broadcasts the RREQ to its neighbours. By a valid route, we mean a route with a high sequence number and lower hop count.

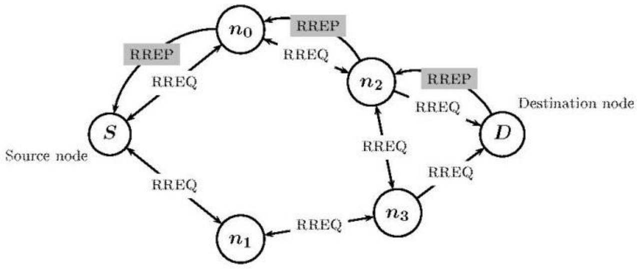
Figure.2.RREP Message



Type	Bits	Prefix	Reserved	Hop Count
DEST Address				
DEST SEQN				
SRC Address				
Lifetime				

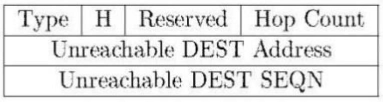
This mechanism is repeated until the RREQ reaches an intermediate node which holds a valid route to the destination or the RREQ reaches the destination node. Thus, a node replies to a RREQ by a RREP in two cases, if it has a fresh route to the destination or if it is itself the destination. The procedure of route construction is depicted in figure 3, where node S broadcasts a RREQ to reach node D. Intermediary nodes n_0, n_1, n_2 and n_3 play in this scenario the role of routers which forward the RREQ **(Kumar, A. et al, 2021)**.

Figure.3.AODV Route Construction Procedure



Established routes are maintained until an error occurs (link break, out of time ...etc). In this case the node which detects the error tries to fix the error locally otherwise it sends a RERR message (depicted in figure 4). After receiving the RERR, the source node initiates a new route establishment procedure **(Kumar, A. et al, 2023)**.

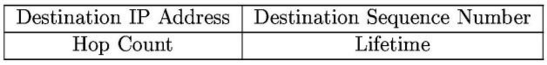
Figure.4.RERR Message



Type	H	Reserved	Hop Count
Unreachable DEST Address			
Unreachable DEST SEQN			

A node maintains connectivity information and an up-to-date neighbours list by broadcasting local Hello messages. Hello messages are broadcast only if the node is part of a valid route. The Hello message is represented in the figure 5 (**Perkins, C., et al, 2003**).

Figure.5. Hello Message



Destination IP Address	Destination Sequence Number
Hop Count	Lifetime

Recent researches, on ad-hoc networks, are focusing on security aspects **(Alzaqebah, A., et al, 2023).** Indeed, although native AODV assures good results for routing, unfortunately it is very vulnerable to attacks, since its programming has been focused on routing aspect without considering security. Vulnerabilities include:

- Open transmission;
- Dynamic topology;
- Any node can freely participates to routing path;
- Absence of a Sink point;
- Need for cooperation between the nodes;
- Heterogeneity of the nodes;
- Limited capacities.

3.Intrusion Detection Systems

Intrusion detection system (IDS) is a mechanism intended to detect abnormal or suspicious activities on the network or a host and to isolate the source of that threats. The effectiveness of these systems is measured by the rapidity of detection of that threats and the speed of isolating them **(de Souza, C. et al, 2022)**. Another important parameter is the false positive cases; an effective IDS detects and isolates malicious nodes and avoids the consideration of trusted activity as malicious **(Alzaqebah, A., et al, 2023)**.

Intrusion detection systems (IDS) play a very important role in networks security. Such systems are implemented to monitor the networks in order to detect suspect activities and to isolate the source of those threats **(Bediya, A. K., & Kumar, R., 2023).**

Intrusion detection systems are often classified into two categories **(Khan, K., et al, 2020)**:

3.1.Signature-based:

Signature-based intrusion detection systems locate potential threats by looking for specific behaviours, such as sequences of bytes in network traffic or sequences of known malicious instructions used by malware. Although these systems are able to easily detect known attacks, they are unable to detect new attacks, for which no pattern is known.

3.2.Anomaly-based:

In this category, systems were designed to detect and adapt to unknown attacks. This approach helps detect unknown attacks. On the other hand, false positives can sometimes be generated, because a legitimate activity can be accidentally classified as malicious activity.

It is also possible to classify IDS according to the target they will monitor, the most common being network intrusion detection systems and host intrusion detection systems. Some IDSs have the ability to respond to the threats they have detected, these response-capable IDSs are intrusion prevention systems.

4. Review of Related Works

Many Intrusion detection systems were proposed to mitigate black holes attacks; each proposed system has its strength points and weakness. To ensure network security, many researchers tried to find techniques to detect and isolate these threats. Black hole attack detection techniques are classified into several categories:

- Based on cryptography **(Dhanaraj, R. K., et al, 2022) (Bandecchi, S., & Dascalu, N., 2021) (Papadogiannaki, E.,, 2022) (Talukdar, M. I., et al, 2021)**.
- Based on sequence number threshold **(Tami, A., et al, 2021)** (**Gurung, S., & Chauhan, S., 2019**) **(Mehdi, S. A., & Hussain, S. Z., 2023) (Ram, A., et al, 2021)**.
- Trust-based **(Gurung, S., & Chauhan, S., 2020) (Kanthimathi, S., & Jhansi Rani, P., 2022) (Huang, Y., & Ma, M., 2023).**
- Based on protocol modification **(Tan, N. D., & Van Tan, L., 2020) (Kurian, S., & Ramasamy, L., 2021**}.
- Based on Artificial Intelligence **(Thanuja, R., & Umamakeswari, A., 2019) (Rani, P., et al, 2022) (Makani, R., & Reddy, B. V. R., 2022) (Sharma, K., et al, 2023)**

A cryptographic paradigm to detect and mitigate black hole attacks is proposed in **(Dhanaraj, R. K., et al, 2022).** According to the authors, the proposed method is declared efficient against the black hole attacks. The major inconvenient is the use of RSA Encryption/Decryption which requires high computing performance, while nodes are defined having limited performances.

In (**Gurung, S., & Chauhan, S., 2019**), the authors propose a dynamic threshold to improve the security and the performance of AODV under black hole attack, but its drawback is using a high routing overhead due to transmission of multiple reply packets by the destination nodes.

(Terai, T., et al, 2020) propose leverage information from neighbouring nodes and create a sequence number threshold based on this information to deal with smart black holes. The authors succeeded in improving the PDR by up to 40% and reducing the ASR by up to 50%. The disadvantage of this proposed method is the modification of the RREP format.

The authors **(Tami, A., et al, 2021)** propose IDS based on fixing a threshold in order to detect the black holes, unfortunately in their proposed work some trusted nodes can be considered as malicious nodes.

A security approach called smart black hole and grey hole mitigation is proposed in **(Arun Raj Kumar, P., 2022)** in order to detect and mitigate both black hole and grey hole nodes using a time series analysis of the dropped packets of each node. According to the authors, the computation of the packet drop distance threshold based on Dynamic Time Warping improves the detection accuracy.

The authors in **(Tan, N. D., & Van Tan, L., 2020)** proposed an intrusion detection system by modifying the AODV protocol with aim of decreasing the effect of the black hole attacks. According to the authors, the proposed solution enhances the PDR and halts this type of threats significantly.

The authors in **(Rani, P., et al, 2022)** have proposed an IDS based on using firefly and artificial neural. According to the authors, the proposed approach enhances the Ad hoc On-Demand Distance Vector routing protocol for combating black hole attacks by leveraging the firefly Algorithm with Artificial Neural Network.

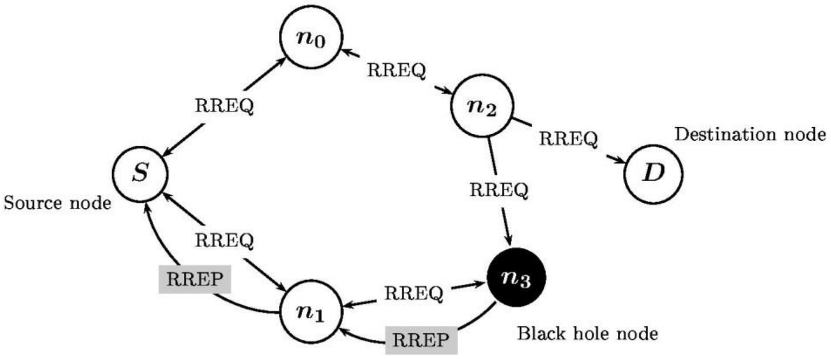
5.Overview of Smart Black Hole

In MANET, no infrastructure is used to initiate and control communications. Nodes are randomly moving, auto configurable and completely autonomous, which make the integration of malicious nodes easier and them detection a difficult task.

Mobile Ad hoc Networks are the object of several attacks, the most dangerous and serious one is the black hole attack, this type attack belongs to denial of service (DoS) attacks in which packets sent from source to destination are discarded or eavesdropped **(Vinayagam, J., et al, 2019)**.

Figure 6 depicts a black hole attack scenario, in which the malicious node n_3, after receiving a RREQ, announces itself as the node that has a fresh route to destination by sending a fake RREP which contains a very high sequence number and low number of hops to the destination.

Figure.6. Black hole attack scenario



By receiving the fake RREP, the source node S (originator of the RREQ) ignores all the other RREP and starts to send data through the route that contains the black hole as an intermediate node. Upon data reception, the black hole drops all received packets instead of forwarding them to the destination, which reduces significantly the network performances **(Mekkaoui.k., Teggar.H., 2023)**.

The black hole attack is classified among the most dangerous threats in MANET, indeed in this attack, a malicious node redirect all communications to itself in order to drop or to modify them, witch hijack the purpose that the network is deployed for. Hence, the necessity to implement an intrusion detection system (IDS) in order to keep the network safe from attacks **(Alzaqebah, A., et al, 2023)**. Many researchers are interested by this field of research and several solutions were proposed in the literature to detect and isolate the black holes, for example by examining the sequence number of the replies **(Tami, A., et al, 2021) (Gurung, S., & Chauhan, S., 2019) (Mehdi, S. A., & Hussain, S. Z., 2023) (Ram, A., et al, 2021)** or by modifying the structure of the AODV control messages **(Tan, N. D., & Van Tan, L., 2020) (Kurian, S., & Ramasamy, L., 2021)** or by sending a RREQ without destination address **(Terai, T., et al, 2020)** since the malicious node responds to all REEQ without checking if the destination address is mentioned in the RREQ or not ... etc. Unfortunately, most of these proposed IDS are now inefficient against the new generation of black holes, known also by smart black holes **(Terai, T., et al, 2020)**.

In the smart black hole attack, a malicious node can defeat several intrusion detection systems **(Terai, T., et al, 2020)**. For example by determining the threshold applied for the sequence number, in the threshold-based IDS which sets a threshold to detect the black holes which announce themselves having a fresh route with a very high sequence number; Or by verifying if the REEQ if it is valid or not by verifying the destination address field in that RREQ.

In this paper, we define a smart black hole as a malicious node that can predict the sequence number threshold, send a fake RREQ, send a fake RREP and check if the received RREQ is valid or notTo determine the sequence number threshold, the least-squares method is used, by exploiting the information collected from neighbours (Terai, T., et al, 2020). The main idea is that the sequence number increases proportionally over time. Therefore, we used the method of least-squares with the destination sequence number and its acquisition time.

5.1.Problem formulation

Consider the sequence numbers $S_1, S_2, ..., S_n$, taken at times $T_1, T_2, ..., T_n$. We define X_n by the equation:

$$X_n = T_n - T_{n-1} \tag{1}$$

This represents the time interval which separates the reception of two consecutive sequence numbers.

We define, also, the two sets X and S by:

$$X = \{X_1 \ , \ X_2 \ , \ X_3 \ , \ \ldots, \ X_n\} \tag{2}$$

and

$$S = \{S_1 \ , \ S_2 \ , \ S_3 \ , \ldots, \ S_n\} \tag{3}$$

With which it is possible to define the equation of a line by:

$$y = Ax + B \tag{4}$$

With

$$A = \frac{COV(X,S)}{\sigma^2 x} \tag{5}$$

$$B = \bar{S} - A\bar{X} \tag{6}$$

Where:

$$COV(X,S) = \sum_{i=1}^{n} \frac{(x_i - \bar{X}) \times (s_i - \bar{S})}{n} \tag{7}$$

is the covariance between X and S;

$$\sigma x = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{X})^2}{n}} \tag{8}$$

Defines the standard deviation of X;

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n} \tag{9}$$

Defines the average of X;

$$\bar{S} = \frac{\sum_{i=1}^{n} S_i}{n} \tag{10}$$

Defines the average of S;

For example, suppose the following sets:

- $X = \{3, 4, 11, 14\}$
- $S = \{5, 6, 20, 29\}$

We can build the following data-sets $(X,S)=\{(3,5),(4,6),(11,20),(14,29)\}$, then:

- $\bar{X}=8$
- $\bar{S}=15$
- $COV(X,S)=\frac{185}{4}$
- $\sigma x=\sqrt{\frac{43}{2}}$

Hence the line equation (4) becomes:

$$y=\frac{185}{86}x-\frac{95}{43} \tag{11}$$

From equation (11), we can predict y with a given x , such that if $x=4$ then $y\approx 6.4$, which is approximately equal to the datum $(4,6)$ in the set (X,S).

By using least-squares method, a smart black hole can predict the destination sequence number at any given time by using the equation (11). With which it can send a fake RREP with the predicted sequence number by adding a small scalar α , because of the predicted threshold must be slightly higher than the real sequence number value. Hence the inefficiency of the threshold-based IDS to detect smart black holes. In general, the threshold value is defined by the following expression:

$$Threshold=Predicted\_SEQ\_Number+\alpha \tag{12}$$

Where:

- *Predicted_SQN_Number* : represents the approximated actual sequence number,
- α is a scalar for preventing the detection of a smart black hole node.

A smart black hole can, also, check if a RREQ is valid or not, since in some trust-based intrusion detection systems and in order to mitigate black hole attacks, a source node, before sending a real RREQ, sends a fake RREQ without a destination number, by receiving this RREQ, a classic black hole replies immediately by a RREP, which contains a very high sequence number and a low hop count, to announce itself the node that has the newest route with the lower hop count, this without checking if the destination number exist or not. However, a smart black hole, and before to reply with a RREP, verifies firstly if the RREQ is valid or not, by checking if the destination address exist in the RREQ or not.

6. Simulations and Results

We used NS2 to evaluate the performances of trust-based and threshold-based intrusion detection systems under smart black hole attacks. NS2 is an event-driven simulator specially designed to study the dynamic nature of wireless communication networks and widely used by researchers.

We simulated Threshold-based and trust-based IDS with different networks, comprising different number of nodes varying from 30 to 100 nodes, under different number of smart malicious node attacks. In this paper, a smart black hole is defined by a malicious node that can defeat trust-based IDS by checking if the RREQ is valid or not, sends a fake RREP and can defeat the threshold-based IDS by predicting the threshold of the sequence number by using the least-squares method.

In our simulations, the initial position of the source node and the destination node are defined on opposite edges of the network. The rest of the nodes are randomly positioned (including the smart black hole nodes). The protocol used is the AODV protocol.

Simulations were carried out with native AODV protocol, AODV with threshold-based IDS and AODV with trust-based IDS with and without smart black holes. We set the packet size to 512 bytes and the simulation time to 200 seconds. The used transport protocol is UDP and the type of traffic used is constant bit rate (CBR). Table 1 shows the simulation parameters. To study the impact of smart black holes on the mentioned intrusion detection systems, we have studied the following metrics: Packet Delivery Ratio (defined in formula 13), End to End Delay (defined in formula 14) and Throughput (defined in formula 15).

Table.1. The simulation parameters.

Parameters	Values
Simulator	NS2.35
Network area	1200 × 1200
Number of nodes	30, 40, 60, 80 and 100
Number of Black holes	1SBH up to 4 SBH
Routing protocol	AODV
Mobility model	Random way point
packet size	512 Byte
Simulation time	200 seconds
Traffic type CBR	Agent UDP

$$\text{PDR} = \frac{\text{Number of received Packets}}{\text{Number of sent Packets}} \times 100 \tag{13}$$

$$\text{End-to-End Delay} = \text{Received time} - \text{Sent time} \tag{14}$$

$$\text{Throughput} = \frac{\text{Number of delivered packets} \times \text{Packet size} \times 8}{\text{Simulation time}} \tag{15}$$

6.1. Case of single attack:

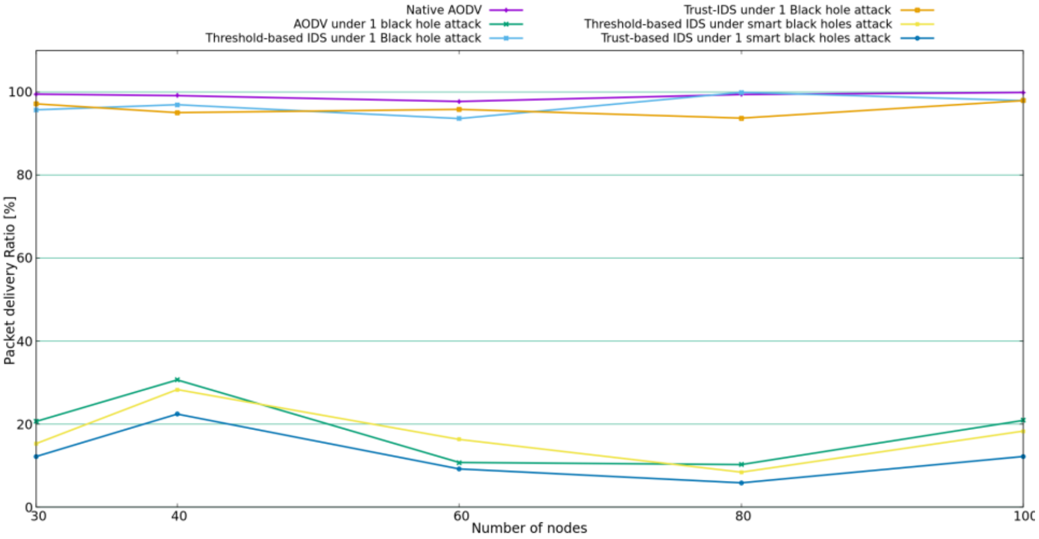
In this case, we simulated the impact of single classic black hole attack and single smart black hole attack on native AODV, Threshold-based IDS and Trust-based IDS. The first studied metric was the packet delivery ratio (PDR), defined in equation 13.

From figure 7, we can conclude that native AODV, without attack, assure a good PDR in the different networks (30, 40, 60, 80 and 100 nodes), on average of 99%; but when a black hole is integrated the PDR is decreased on average of 75%, This because of the black hole that drops the received packets after redirecting the communication to itself by sending a fake RREP with a very high sequence number.

The PDR is enhanced after applying Threshold-based IDS, on average of 95%, this is due to the use of threshold for the sequence number to detect the malicious node; But This IDS is unable to detect the smart black hole that use the least-squares method to predict the applied threshold by this IDS. The simulated threshold-based IDS, under smart black hole attack, showed great weakness against this attack, indeed the measured PDR was on average of 15%.

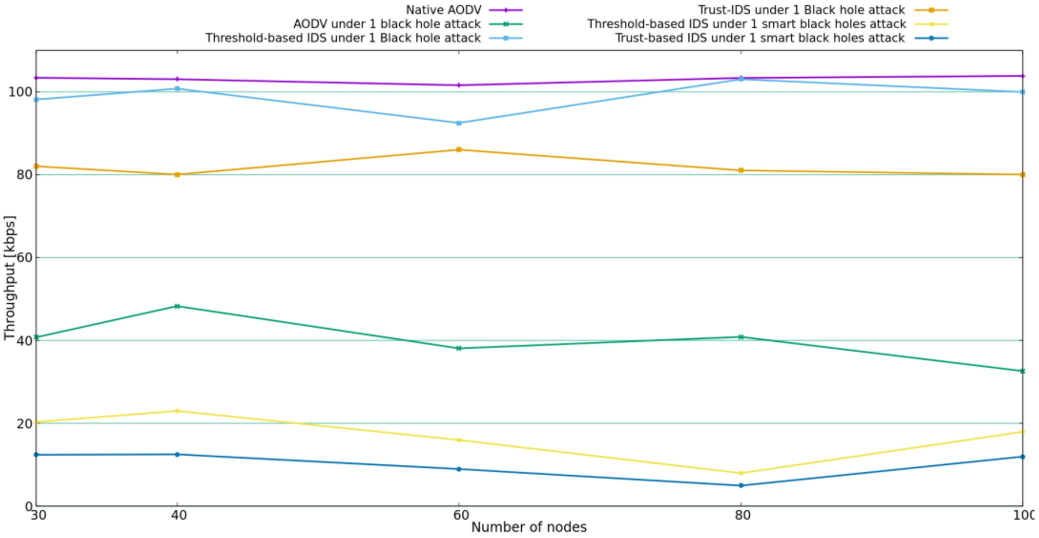
We can conclude, also, from figure 7, that the Trust-based IDS keeps the networks safe against the classic black hole attack, by enhancing the PDR on average of 95%. This is due by isolating the nodes that reply to the fake RREQ by a RREP. This IDS is unable to detect the smart black hole, because in this attack the malicious node check the validity of the received RREQ by verifying the destination address before replying.

Figure.7.impact of single attack on PDR



The second studied metric in this paper is the average throughput. From figure 8, we can conclude that native AODV operates the networks with the maximum throughput, around 103 kbps, but after integrating of a black hole the measured throughput was around 40 kbps, i.e. a deterioration of 60%. The throughput is enhanced after applying the threshold-based IDS and trust-based IDS, which mitigate the black hole attack. The throughput recorded after applying of threshold-based IDS was around 99 kbps, whereas the throughput recorded after applying the trust-based IDS was around 80kbps, this is due the used mechanism to detect threats.

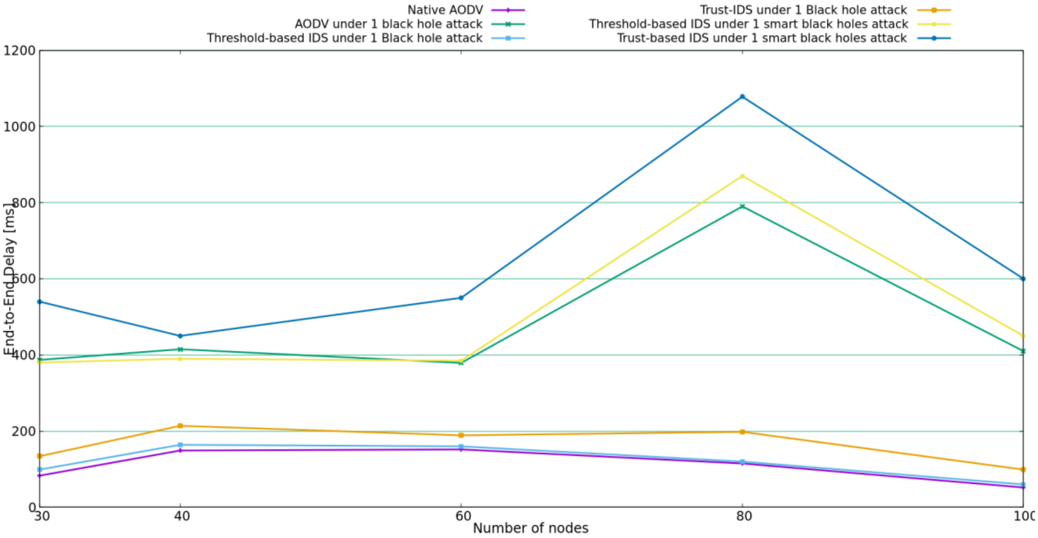
Figure.8.impact of single attack on throughput



We can, also, conclude from figure 8, that both IDS, trust-based and threshold-based, are inefficient against smart black hole attack. Indeed, the throughput recorded by the IDS was, respectively, around 15kbps and 20 kbps, this is due to the incapacity of these IDS to detect and isolate the smart malicious node.

The impact of a single attack on the end-to-end delay (E2ED) is depicted in figure 9. From the figure we can note that native AODV minimize the E2ED which represents the time taken for a packet to be transmitted across a network from source to destination, this time becomes very high when a black hole is injected in the network and varies between 400ms and 1200ms. Threshold-based and Trust-based IDS can mitigate the impact of classical black hole and assure minimal end-to-end delay. But when a smart black hole in integrated in the networks the two IDS stay inefficient against this smart malicious node.

Figure.9.impact of single attack on End-to-End Delay



6.2.Case of multiple attack

In this scenario, multiple classical and smart black hole attacks are simulated with networks of different densities (30, 40, 60, 80 and 100 nodes). Figure 10 depicts the impact of these attacks on the PDR. From the figure we can note that the measured PDR in native AODV is on average of 99%. But when the malicious nodes (5 black holes) are integrated the PDR decreases with an average of 100% to be 0% (no packet was delivered). To mitigate these black holes, two IDS were applied; threshold-based and trust based IDS, so the PDR is enhanced by an average 95%. Form the figure we can note, also, that these IDS are inefficient against the smart black holes which decreases the PDR to be 0%.

Figure.10.impact of multiple attacks on PDR

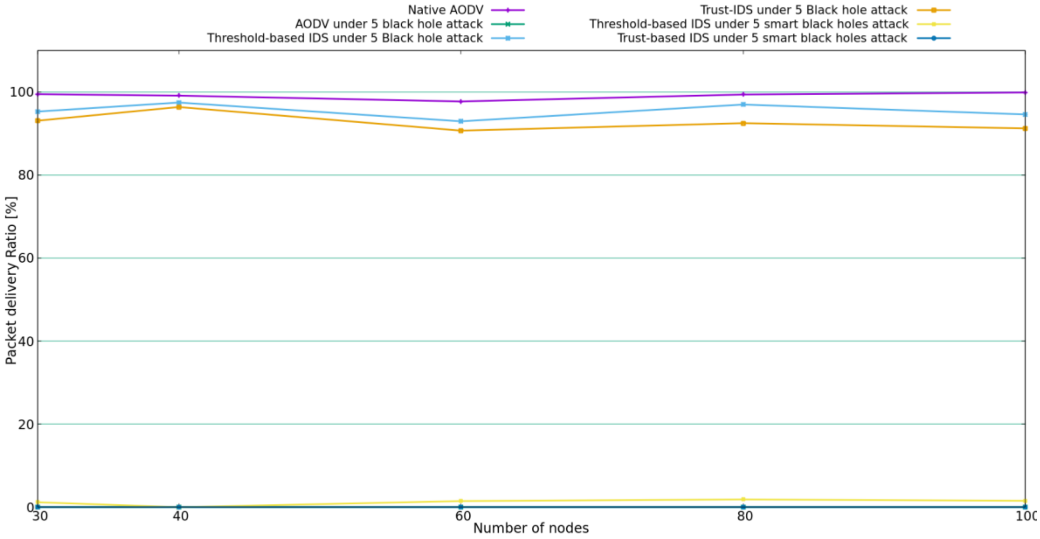
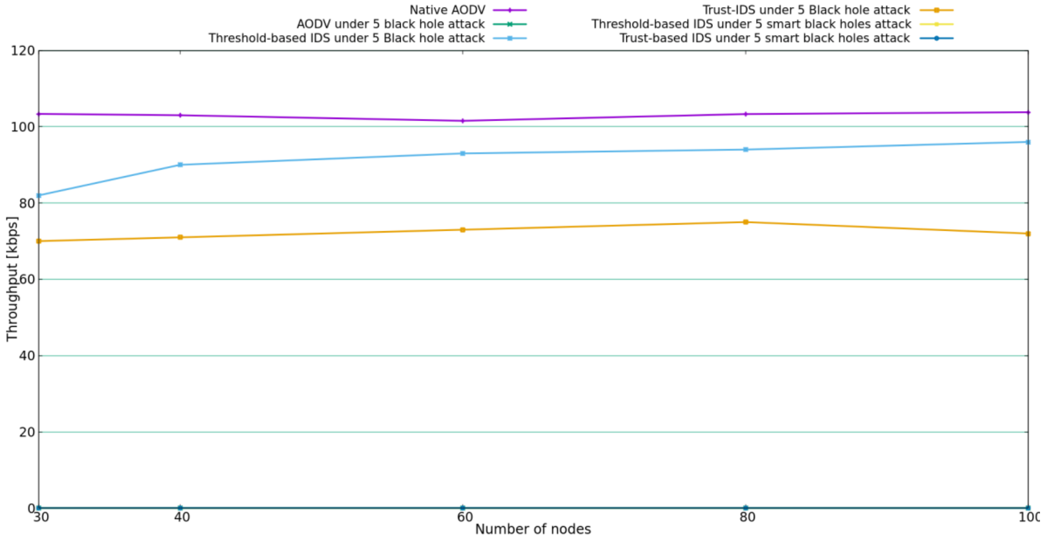


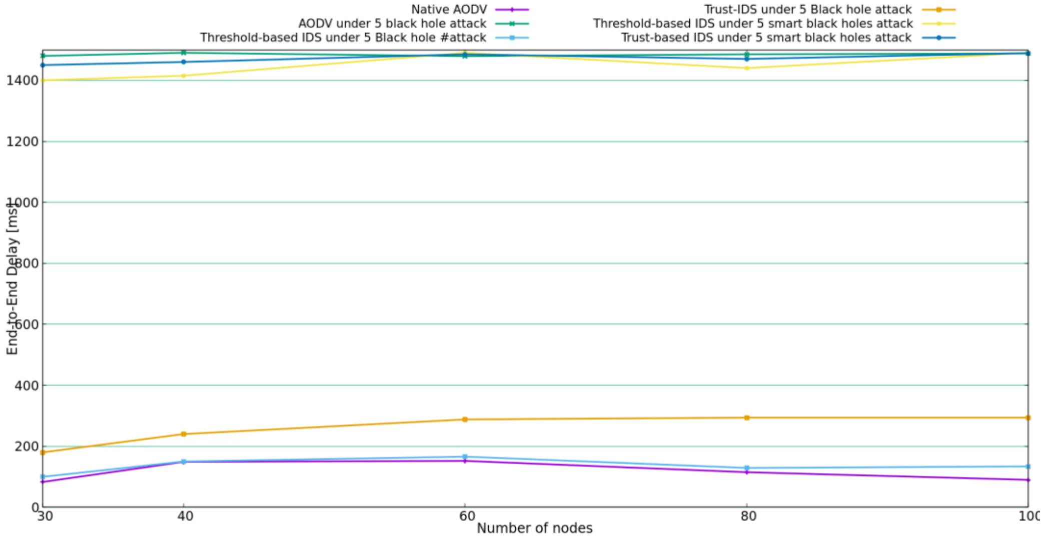
Figure 10 shows the impact of the smart malicious nodes on the average throughput. We can conclude that native AODV operates the networks with the maximum throughput, around 103 kbps, but after integrating five black holes the measured throughput decreases to around 0 kbps, i.e. a deterioration of 100%. The throughput is enhanced after applying the threshold-based IDS and trust-based IDS, which mitigate the black hole attack. The throughput recorded after applying of threshold-based IDS was around 90 kbps, whereas the throughput recorded after applying the trust-based IDS was around 70kbps, this is due the used mechanism to detect threats and the time between sending a fake RREQ and receiving RREP.

Figure.11.impact of multiple attacks onThroughput



The impact of a single attack on the end-to-end delay (E2ED) is depicted in figure 12. From the figure we can note that native AODV minimize the E2ED, this time becomes very high when multiple black holes are injected in the network and varies between 1450ms and 1500ms. Threshold-based and Trust-based IDS can mitigate the impact of classical black hole and assure minimal end-to-end delay. But when a smart black hole in integrated in the networks the two IDS stay inefficient against this smart malicious node.

Figure.12.impact of multiple attacks on End-to-End Delay



7. Conclusion

Mobile Ad hoc networks (MANETs), known to be self-configured, non-infrastructure and peer networks, are subject to multiple types of attacks. Hence, it is essential to implement Intrusion Detection System (IDS) to realize fast attack detection and to alert users by any malicious activity. The most serious and dangerous threats in MANETs is Black hole attack, which is the origin of Denial of service. This type of threats has been largely studied and many IDS were proposed. Unfortunately these solutions have become inefficient against the new generation of black holes, known also by smart black holes, which can deceive most of these solutions. In this paper, we studied the impact of two widely used IDS, threshold-based IDS and Trust-based IDS. Simulations made under network simulator NS 2.35 showed that smart black holes defeat these IDS and decrease significantly the network performances, thus the necessity to find new IDS to mitigate these smart attacks.

References

AlKhatieb, A., Felemban, E., & Naseer, A. (2020, April). Performance evaluation of ad-hoc routing protocols in (FANETs). In 2020 IEEE wireless communications and networking conference workshops (WCNCW) (pp. 1-6). IEEE.

Al Rubaiei, M. H., Jassim, H. S., & Sharef, B. T. (2022). Performance analysis of black hole and worm hole attacks in MANETs. International Journal of Communication Networks and Information Security (IJCNIS), 14(1).

Alzaqebah, A., Aljarah, I., & Al-Kadi, O. (2023). A hierarchical intrusion detection system based on extreme learning machine and nature-inspired optimization. Computers & Security, 124, 102957.

Arega, K. L., Raga, G., & Bareto, R. (2020). Survey on performance analysis of AODV, DSR and DSDV in MANET. Computer Engineering and Intelligent Systems, 11(3), 23-32.

Arun Raj Kumar, P. (2022). Detection and Mitigation of Smart Blackhole and Gray Hole Attacks in VANET Using Dynamic Time Warping. Wireless Personal Communications, 124(1), 931-966.

Bandecchi, S., & Dascalu, N. (2021). Intrusion Detection Scheme in Secure Zone Based System. Journal of Computing and Natural Science, 19-25.

Bediya, A. K., & Kumar, R. (2023). A novel intrusion detection system for internet of things network security. In Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 330-348). IGI Global.

Bhati, N. S., Khari, M., García-Díaz, V., & Verdú, E. (2020). A review on intrusion detection systems and techniques. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 28(Supp02), 65-91.

Bhushan, B., & Sahoo, G. (2019). Routing protocols in wireless sensor networks. In Computational intelligence in sensor networks (pp. 215-248). Springer, Berlin, Heidelberg.

Bolla, D. R., Naidu, P. R., JJ, J., TR, V., & Palle, S. S. (2023). Energy-Efficient Dynamic Source Routing in Wireless Sensor Networks. In Emerging Research in Computing, Information, Communication and Applications (pp. 749-763). Springer, Singapore.

Cheng, Y., Cetinkaya, E. K., & Sterbenz, J. P. (2012, March). Dynamic source routing (DSR) protocol implementation in ns-3. In Proceedings of the 5th international ICST conference on simulation tools and techniques (pp. 367-374).

de Souza, C. et al (2022). Intrusion detection and prevention in fog based IoT environments: A systematicliterature review. Computer Networks, 109154.

Dhama, S. et al (2016, March). Black hole attack detection and prevention mechanism for mobile ad-hoc networks. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 2993-2996). IEEE.

Dhanaraj, R. K., Islam, S. K., & Rajasekar, V. (2022). A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments. Wireless Networks, 28(7), 3127-3142.

Gurung, S., & Chauhan, S. (2019). A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Networks, 25(4), 1685-1695.

Gurung, S., & Chauhan, S. (2020). A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. Wireless Networks, 26(3), 1981-2011.

Huang, Y., & Ma, M. (2023). Ill-ids: An incremental lifetime learning ids for vanets. Computers & Security, 124, 102992.

Kanthimathi, S., & Jhansi Rani, P. (2022). An efficient packet dropping attack detection mechanism in wireless ad-hoc networks using ECC based AODV-ACO protocol. Wireless Networks, 1-13.

Kariyannavar, S. S. et al (2021, January). Security in Mobile ADHOC Networks: Survey. In 2021 6th International Conference on Inventive Computation Technologies (ICICT) (pp. 135-143). IEEE.

Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture, 105, 101701.

Kumar, A., Shukla, R. K., & Shukla, R. S. (2023). Survey of Comparative Analysis of Different Routing Protocols in MANETs: QoS. Cyber Technologies and Emerging Sciences, 419-424.

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., ... & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems, 80, 103352.

Kurian, S., & Ramasamy, L. (2021). Novel AODV based service discovery protocol for MANETS. Wireless Networks, 27(4), 2497-2508.

Makani, R., & Reddy, B. V. R. (2022). Designing of Fuzzy Logic-Based Intrusion Detection System (FIDS) for Detection of Blackhole Attack in AODV for MANETs. In Cyber Security and Digital Forensics (pp. 113-128). Springer, Singapore.

Mehdi, S. A., & Hussain, S. Z. (2023). Survey on Intrusion Detection System in IoT Network. In International Conference on Innovative Computing and Communications (pp. 721-732). Springer, Singapore.

Mekkaoui, K., & Teggar, H. (2023). Mitigation of smart black hole attacks using universal sink detection in graph theory. The journal of supercomputing (under reviewing).

Papadogiannaki, E., Tsirantonakis, G., & Ioannidis, S. (2022, June). Network intrusion detection in encrypted traffic. In 2022 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.

Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. rfc3561).

Rajeswari, A. R. (2020). A mobile Ad hoc network routing protocols: a comparative study. Recent Trends in Communication Networks, 1-24.

Ram, A., Kulshrestha, J., & Gupta, V. (2021). Secure Routing-Based AODV to Prevent Network from Black Hole Attack in MANET. In Proceedings of 6th International Conference on Recent Trends in Computing (pp. 633-642). Springer, Singapore.

Rani, P., Verma, S., Rawat, D. B., & Dash, S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications, 1-11.

Sharma, K., Chawla, M., & Tiwari, N. (2023). Intrusion detection system using machine learning approach: A review. In International Conference on Innovative Computing and Communications (pp. 727-734). Springer, Singapore.

Soomro, A. M., Fudzee, M. F. B. M., Hussain, M., Saim, H. M., Zaman, G., Atta-ur-Rahman, H. A., & Nabil, M. (2022). Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management. Journal of Communications, 17(9).

Talukdar, M. I., Hassan, R., Hossen, M. S., Ahmad, K., Qamar, F., & Ahmed, A. S. (2021). Performance improvements of AODV by black hole attack detection using IDS and digital signature. Wireless Communications and Mobile Computing, 2021.

Tami, A., Boukli Hacene, S., & Ali Cherif, M. (2021). Detection and prevention of blackhole attack in the AOMDV routing protocol. Journal of Communications Software and Systems, 17(1), 1-12.

Tan, N. D., & Van Tan, L. (2020). IMPLEMENTATION OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOLS IN MANET USING NS2. UTEHY Journal of Science and Technology, 25, 45-51.

Terai, T., Yoshida, M., Ramonet, A. G., & Noguchi, T. (2020, November). Black hole Attack Cooperative Prevention Method in MANETs. In 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW) (pp. 60-66). IEEE.

Thanuja, R., & Umamakeswari, A. (2019). Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. cluster computing, 22(2), 3131-3143.

Thamizhmaran, K., & CHARLES, A. (2022). Comparison of On-Demand Routing Protocol for MANET using Simulation. i-manager’s Journal on Communication Engineering and Systems, 11(1), 13-18.

Quy, V. K. et al (2021). A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications, 120(1), 49-62.

Vinayagam, J., Balaswamy, C. H., & Soundararajan, K. (2019). Certain investigation on MANET security with routing and blackhole attacks detection. Procedia Computer Science, 165, 196-208.

Zaatouri, I., Sailhan, F., Rovedakis, S., Guiloufi, A., Alyaoui, N., & Kachouri, A. (2019, March). Performance Evaluation of Mobility-Aware Routing Protocol for Low power and Lossy Networks. In 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 636-641). IEEE.