Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 236 (2024) 177–184

Procedia Computer Science

www.elsevier.com/locate/procedia

International Symposium on Green Technologies and Applications (ISGTA'2023)

Kolmogorov-Smirnov based method for detecting black hole attack in vehicular ad-hoc networks

Badreddine Cherkaoui[a*], Mohammed-Alamine El Houssaini[b], Mohammed Kasri[c], Abderrahim Beni-Hssane[c], Mohammed Erritali[d]

[a]*LAROSERI Laboratory, Mathematics and Computer Science Department, High School of Technology, Chouaïb Doukkali University, Sidi Bennour, Morocco*
[b]*ESEF, Chouaib Doukkali University, El Jadida, Morocco*
[c]*LAROSERI Laboratory, Computer Science Department, Facultyof Sciences Chouaïb Doukkali University, El Jadida, Morocco*
[d]*TIAD Laboratory, computer science department, Sciences and Technics Faculty, University of Sultan Moulay Slimane, Béni-Mellal, Morocco.*

Abstract

The security of ad hoc networks continues to pose a major challenge in today's digital age. Threatened by unscrupulous users, especially in decentralized and open architectures, ad-hoc vehicular networks make protection against malicious attacks a difficult task. Vehicular networks, a specific subset of ad hoc networks, inherit security vulnerabilities from their parent network. One of the best-documented attacks is the black hole, in which a malicious user attempts to manipulate the routing mechanism to gain unauthorized access to the route, then intercepts and discards data packets. The result is an interruption of service to the intended recipient. In our research, we propose a black hole attack detection system based on the Kolmogorov-Smirnov statistical method. This system is designed to identify communication disruptions caused by such attacks without requiring structural modifications to the routing protocol. The results show that the proposed method can detect the presence of the attack by monitoring network activity. The results are tested and validated using SUMO (Simulation of Urban MObility) to generate microscopic road traffic, and NS-2 (Network Simulator) to generate network communication.

Peer-review under responsibility of the scientific committee of the International Symposium on Green Technologies and Applications

Keywords: **Kolmogorov-Smirnov, VANET, Black hole attack;**

1. Introduction

VANETs have seen significant growth, with various standards, applications, and routing mechanisms proposed to address their unique requirements. Key challenges include the high mobility of vehicles, spatiotemporal variations in traffic density[1], and the absence of infrastructure for wireless communication. Security is a major concern in VANETs, with a focus on securing communication and data management. One widely discussed routing protocol in

Peer-review under responsibility of the scientific committee of the International Symposium on Green Technologies and Applications
10.1016/j.procs.2024.05.019

VANETs is AODV[2], which assumes honest behavior from all network nodes and lacks built-in security mechanisms. As a result, data routed through AODV is vulnerable to threats like Denial of Service (DOS)[3] attacks, including the blackhole attack[4], which disrupts communication by forging routing information. To counter blackhole attacks, various countermeasures are proposed, often involving modifications to the AODV protocol structure. However, these changes impact the overall processing time and network latency. Researchers aim to minimize protocol changes during the detection and reaction phases.

In this paper, the proposed method employs the Kolmogorov-Smirnov (K-S) normality test to monitor the network activity and then identify possible anomalies caused by the black hole attack. The paper is organized into five parts: the introduction being the first. Then, an overview of routing protocols and solutions for detecting blackhole attacks as a second part. The third part is about a theoretical study of the proposed detection method. The fourth part is dedicated for an evaluation and experimentation section using real map data in a urban VANET environment. The final part is a summary of our presented work with potential future directions.

2. Background

2.1. View of the treated problem

AODV (On Demand Distance Vector) is a reactive routing protocol that discovers and maintains paths when needed. When a node wants to send data to another, it broadcasts a route request (RREQ) message to find a route. Nodes along the way update the path and reply with a route reply (RREP) message[5]. The routing path is a chain of nodes, and packets are forwarded using pointers. AODV operates in a distributed manner, with each node maintaining only its adjacent pointers. The protocol uses route time-out, Hello messages, and route error (RRER) messages to maintain the path and detect link breaks. The figure Fig. 1(a) illustrate the explained mechanism of AODV routing protocol.

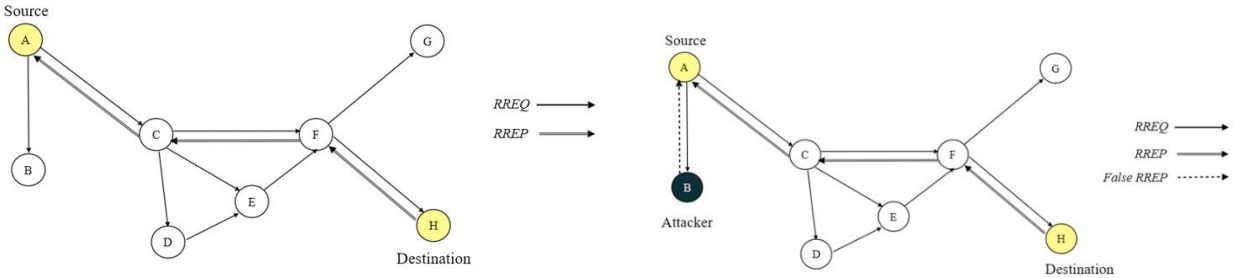

Fig. 1: (a) AODV routing protocol mechanism, (b) Black hole attack acting mechanism[6]

As shown in figure Fig. 1(b), a malicious node attempts to attract and control data traffic in the network by manipulating routing information. When it receives a route request (RREQ) from a source node, the malicious node responds with a fake route reply (RREP) claiming to have the shortest path to the destination. This false route is selected for data transfer, allowing the malicious node to intercept and discard the data packets, preventing their reinsertion into the network. This attack disrupts the network by forcing the receiver node into an out-of-service mode and significantly reducing network throughput. The impact of the attack depends on the attacker's location, with strategic locations having a greater impact, especially in dynamic networks like VANET. In such cases, the attacker can mimic normal node behavior, making detection more challenging.

2.2. Related work

Vehicular ad-hoc networks are a usual subject to multiple vulnerabilities such as the black hole attack. These are some of the best works which discuss this issue:

In this study[7], the authors present an approach for addressing the Black Hole attack within a MANET setting. Their method involves deploying an algorithm that fosters collaboration among nodes to monitor the data packet transmission at the subsequent node. This observation process is initiated by the source node. If a transmission error is detected, the observing node promptly sends an error message back to the source node. In the event that the source node receives multiple error messages, it identifies the observed intermediate node as a potential black hole. What sets this approach apart is its ability to minimize alterations to the routing protocol, thus preventing undue network congestion.

In[8], the authors introduce an approach called "Detecting and Preventing a BHA" (DPBHA) to enhance security and optimize the performance of VANET networks. Their objective is to detect malicious behavior during the initial route discovery phase. The proposed method involves dynamically calculating a threshold value and generating a deceptive route request (RREQ). This methodology is subsequently implemented and assessed using the NS-2 simulator, with the primary evaluation metric being the Packet Delivery Ratio (PDR). It's worth noting that this study does not delve into the implications of a high number of nodes operating within an urban environment.

S. Gurung and S. Chauhan[9] have introduced a modification to the AODV protocol, which they have aptly named MBDP-AODV, to accommodate their approach for dynamic sequence number assignment. In this method, the sending node determines the dynamic sequence number threshold by computing the mean and standard deviation of destination sequence numbers from multiple response packets. Should a suspicious packet with an uncertain sequence number be detected, the source node forwards this packet to the next hop in an effort to trace its origin within the network. In cases where an uncertain sequence number is combined with a hop count of 1, the node responsible for the packet is considered a potential malicious actor. Consequently, an alert packet is broadcast to all nodes in the network, effectively preventing the malicious node from participating in any route discovery processes. This approach was validated using the NS-2 simulator, and the results demonstrate its efficacy in mitigating the impact of black hole attacks in MANET environments.

In [4], the authors introduced a novel approach for the real-time detection of black hole attacks within the context of a VANET. This method involves the continuous monitoring of network activities to promptly identify black hole attacks. The foundation of this approach is rooted in statistical process control (SPC), primarily focusing on the observation of packet loss rates. Utilizing control charts, the system analyzes the network's normal behavior to establish upper and lower thresholds for acceptable packet loss rates. Real-time graphical representations of network activities enable the timely identification of black hole attacks. Notably, this method boasts the advantage of not necessitating any modifications to IEEE standards or adjustments to the routing protocol structure.

In[10] Kumar and al. introduce a trust management system and a hybrid optimization algorithm aimed at identifying and thwarting black hole attacks within VANETs. This system comprises two distinct phases: detection and prevention. During the detection phase, the trust management system assesses the reliability of each vehicle in the network, taking into account their historical behavior and communication patterns. In the prevention phase, a hybrid optimization algorithm is employed to determine the most optimal data transmission route while avoiding black hole nodes. To assess the effectiveness of their approach, the authors conducted simulations using the NS-2 simulator, revealing its capability to efficiently detect and prevent black hole attacks in VANETs. However, it is worth noting a limitation in the study, as the authors did not provide a comparative analysis of their system against other state-of-the-art solutions for detecting and preventing black hole attacks in VANETs. This absence of comparison limits the ability to evaluate its effectiveness in relation to alternative approaches.

In conclusion, numerous methods for identifying and mitigating black hole attacks are documented in the literature. Many of these methods employ algorithms to monitor the conduct of nodes within an ad-hoc network, necessitating substantial adjustments to the routing protocol structure or even the underlying IEEE standard. These alterations may have consequences for routing protocol performance, subsequently affecting network performance by introducing delays or overload. In our paper, we have adopted an alternative approach, employing a statistical method to monitor network behavior under typical conditions. Notably, this method does not demand any modifications to the AODV protocol, preserving the protocol's original structure.

3. The proposed method

3.1. Kolmogorov-Smirnov test

The Kolmogorov-Smirnov (K-S)[11] test is designed to identify disparities between distributions. It does so by assessing the maximum difference between empirical distribution functions. In the test, the maximum discrepancy between two cumulative probabilities, denoted as D, is used. To perform the K-S test [12], an estimate of the distribution function is generated from the observed sample for comparison with the distribution function of a theoretical law. This estimation process begins with the arrangement of sample values X_i, traditionally termed order statistics. The empirical distribution function is defined as follows:

$$\widehat{F_n} = \begin{cases} 0 \; for \; x < X_n \\ \dfrac{i}{n} \; for \; X_i \leq x < X_{i+1} \\ 1 \; for \; x \geq X_n \end{cases} \tag{1}$$

Hence, the estimation of F(x) = P ($X \leqslant x$) involves determining the proportion F(x) of sample elements that are less than or equal to the value x. The fundamental idea behind the test is that when the null hypothesis H_0 is valid, the empirical distribution function $\hat{F}$ derived from the sample should closely resemble F.

Let's consider a scenario with observations $X_1, X_2, ..., X_n$, which are believed to follow a distribution P. The testing procedure involves making a decision to either reject or, rarely, accept a statistical hypothesis known as the null hypothesis ($\boldsymbol{H_0}$). This decision is based on the data provided by the sample, and it involves evaluating both the null hypothesis $\boldsymbol{H_0}$ and an alternative hypothesis $\boldsymbol{H_1}$, as follows:

$\boldsymbol{H_0}$: The samples come from P
Against
$\boldsymbol{H_1}$: The samples do not come from P

In our context, we aim to assess the normality of two sample sets. To do so, we work with two distinct and independent sets of samples: $X_1, X_2, ..., X_n$, each following an identically distributed distribution function F0, and $Y_1, Y_2, ..., Y_m$, which follow the same distribution function F_1. Our objective is to conduct a hypothesis test, comparing $\boldsymbol{H_0}$: $F_0 = F_1$ against $\boldsymbol{H_1}$: $F_0 \neq F_1$. This test involves a comparison of the graphical representations of the data from these two distributions. It computes the maximum separation between the two curves and subsequently derives a *p-value*. A *p-value* exceeding the chosen confidence level α suggests that both datasets adhere to the same normal distribution. Conversely, a *p-value* below the selected α indicates that the two distributions do not exhibit the same normal pattern. The interpretation is that if the p-value is high, the data samples are considered normal. Conversely, a low *p-value* may indicate abnormal network activity, potentially indicating the presence of a black hole attack. The specific *p-value* calculation considers the chosen confidence level α and the sample sizes within each distribution.

3.2. Global strategy

In the context of VANET communication, various factors come into play, influencing the network's performance. One critical factor is the mobility speed of nodes, leading to a continually changing network topology and subsequent performance variations. Additionally, external events, such as the blackhole attack (as discussed in section 2.1), introduce further variability. The blackhole attack is a malicious attempt to intercept network traffic, diverting data packets from their source node. Instead of routing them to their intended destination, the attacker discards these packets. This results in the destination node going out of service due to the loss of packets, directly impacting the overall network performance. The challenge lies in distinguishing between normal and abnormal events. As discussed in section 2.1, the blackhole attack's primary impact is on network throughput, causing a significant decrease. Therefore, our approach revolves around implementing the K-S normality test to monitor the communication process

and identify potential blackhole attacks. The key steps of our overall strategy are visualized in the flowchart provided in Fig. 2:

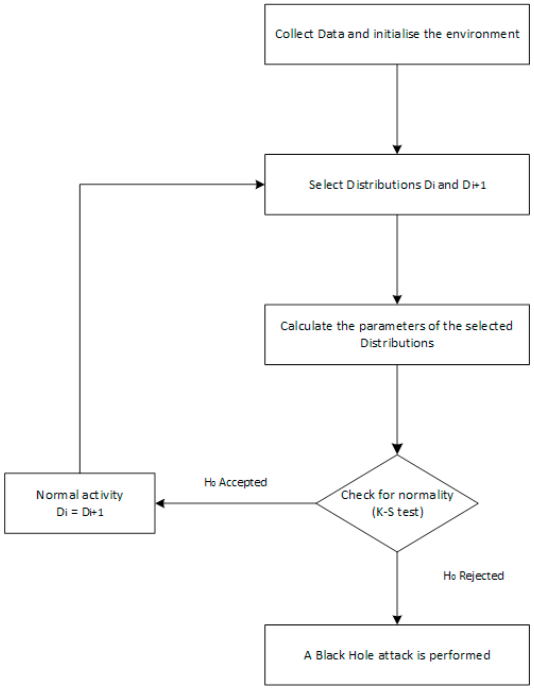

Fig. 2: Global strategy flowchart for detecting the black hole attack

4. Simulations and results

4.1. Simulation tools and environment

To evaluate the effectiveness of our approach, the NS-2 simulator is used for testing purposes. The mobility model was generated using the SUMO microscopic traffic simulator. Our experimentation network represents the urban environment of Fez city, as depicted in Figure 6. This network incorporates multiple entry points that facilitate vehicle access and establish a vehicular flow, mirroring the actual characteristics of Fez city. These characteristics encompass factors like speed limits, traffic signals, roundabouts, road capacities, and traffic directions, thus generating statistics that closely resemble real-world scenarios. This realism enhances the credibility of our detection method. It's essential to note that we excluded factors like hardware failures and deliberate manipulations that could potentially disrupt communication. In our simulations, all communication disturbances are attributed solely to the black hole attack, which we have integrated into our simulator. The primary simulation parameters are summarized in Table I:

TABLE I: Simulation parameters

Parameters	Values
Number of Vehicles	200
Version of the simulator	NS-2.35
Graph construction Tool	Microsoft Excel 2010
Vehicles speed	From 0 to 15m/s
Packet Size	1500
Transmission throughput	5 Mb/s
Traffic Model	CBR Constant Bit Rate
Routing Protocol	AODV
Number of Attackers	1
Simulation Time	400 s

Fig. 3: Map of Fes City in SUMO

4.2. Results and discussion:

This section is dedicated to the performance assessment of our network, aiming to validate the proposed method mentioned earlier. Our VANET network consists of 200 vehicles, with three vehicles in the transmission state and one in the receiving state. Communication initiates at the fourteenth second and continues until the end of the simulation. At the 230th second, a malicious node is introduced, and we subsequently monitor the network's activity by analyzing the overall throughput. The metric chosen to evaluate network performance is the global throughput. The Fig. 4 provides a visual representation of the results observed throughout the simulation duration.

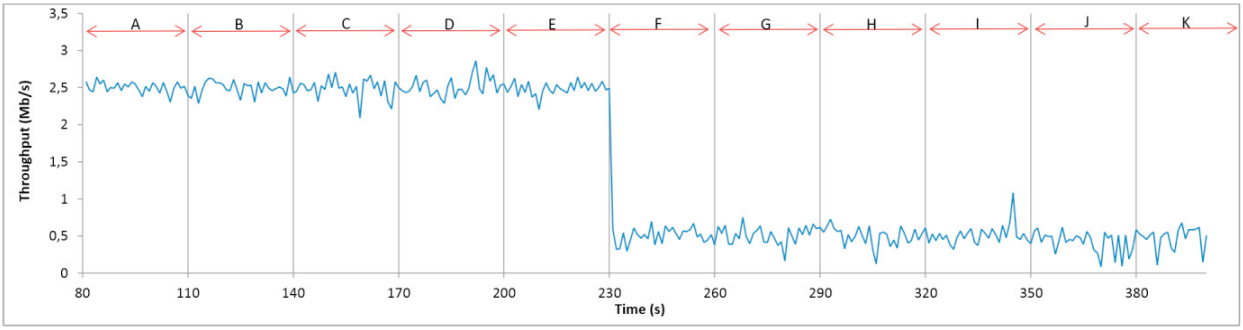

Fig. 4: Network instantaneous throughput

As depicted in Fig. 4, the network throughput experiences a decline following the activation of the black hole attack. This decline indicates that the attack has impacted at least one of the three transmitting nodes. Consequently, the communication between various network components involved in the communication process is no longer operating at an optimal level.

In our testing using the K-S method, we require distributions that contain a minimum of 30 samples. To fulfill this requirement, we activate the black hole attack after the initial 30 seconds of communication. The distribution F_n, representing this period, will be compared with the subsequent distribution, $F_n + 1$. If the K-S test verifies the normality of the data, F_{n+1} becomes the new reference for comparison with the next distribution. This implies that $F_n = F_{n+1}$, signifying that the two distributions are statistically similar.

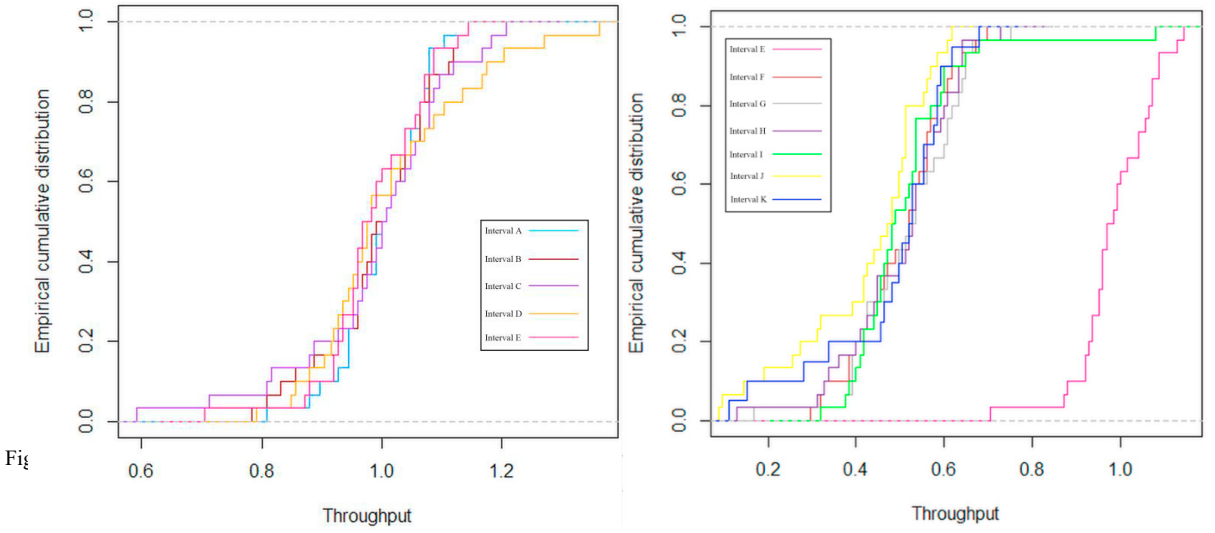

Fig. 5: (a) Kolmogorov-Smirnov test in the normal case, (b) Kolmogorov-Smirnov test in the attack case

TABLE II: Kolmogorov-Smirnov Test

KS test elements	D-value	p-value	α = 0,05
(A, B)	**0.1**	**0.9983**	**0.24**
(B, C)	**0.13333**	**0.9525**	**0.24**
(C, D)	**0.16667**	**0.799**	**0.24**
(D, E)	**0.16667**	**0.799**	**0.24**
(E, F)	**1**	**1.87E-13**	**0.24**
(E, G)	**1**	**1.87E-13**	**0.24**
(E, H)	**1**	**1.87E-13**	**0.24**
(E, I)	**1**	**1.87E-13**	**0.24**
(E, J)	**1**	**1.87E-13**	**0.24**
(E, K)	**1**	**7.55E-11**	**0.24**

The results presented in Fig. 5a, 5b, and Table 2 involve the evaluation of the null hypothesis H_0, which posits that the data within intervals A, B, C, D, and E adhere to a normal distribution pattern. The *p-values* within these intervals range from 0.7 to 0.99, exceeding the calculated confidence level of 0.05. Consequently, we cannot reject the null hypothesis $\boldsymbol{H_0}$, signifying that network activity is within normal parameters. However, in the case of interval *F*, the *p-value* falls below the 0.05 confidence level, leading to the rejection of the null hypothesis $\boldsymbol{H_0}$. This indicates the presence of abnormal network activity. As per our predefined scenario and parameters, this anomaly can be attributed to the black hole attack. Notably, interval E serves as the last known trusted interval, and the subsequent intervals, namely G, H, I, J, and K, all exhibit *p-values* below the significance threshold of 0.05, signaling deviations from the normal pattern.

In this paper, we have proposed a method based on the Kolmogorov-Smirnov statistical test for detecting black hole attacks. This test is a powerful and efficient tool, allowing us to supervise network activity in real time. The advantage of our method is that it is based on a single metric, so no modifications are required to the structure of the studied routing protocol, or to the 802.11p standard. This makes our method more efficient and less computationally-intensive to detect the attack.

5. Conclusion:

Vehicular networks offer substantial potential for enhancing road safety, supporting assisted and autonomous driving, and mitigating the risks associated with human error in driving. Therefore, the imperative objective is to establish reliable and secure communication within this highly critical domain. This research delves into the issue of the black hole attack within vehicular networks and its detrimental consequences. Subsequently, we present a detection approach centered on the Kolmogorov-Smirnov statistical method to identify the presence of such attacks in this context. An advantageous aspect of our detection method lies in its compatibility with existing IEEE standards and routing protocols, highlighting its non-disruptive nature. As perspectives, we are designing a rection method to concatenate the method presented in this article. This will enable us to present a complete system for detecting and reacting against blackhole attacks in VANET environments.

References

[1] A. Ghaffari, "Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks," *J. Ambient Intell. Humaniz. Comput.*, no. 123456789, 2019.

[2] A. A. Chavan, D. S. Kurule, and P. U. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack," *Procedia Comput. Sci.*, vol. 79, pp. 835–844, 2016.

[3] D. Dave and P. Dave, "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET," *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 1690–1696, 2014.

[4] B. Cherkaoui, A. Beni-Hssane, and M. Erritali, "Black hole attack detection in vehicular ad hoc networks using statistical process control," *Int. J. Commun. Antenna Propag.*, vol. 7, no. 3, 2017.

[5] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 133–139, 2017.

[6] B. Cherkaoui, A. Beni-hssane, and M. Erritali, "Variable control chart for detecting black hole attack in vehicular ad-hoc networks," *J. Ambient Intell. Humaniz. Comput.*, Mar. 2020.

[7] Y. M. Khamayseh, S. A. Aljawarneh, and A. E. Asaad, "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency," *Sustain. Comput. Informatics Syst.*, vol. 18, pp. 90–100, 2018.

[8] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J. T. Seo, "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs," *Sensors (Basel).*, vol. 22, no. 5, pp. 1–27, 2022.

[9] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wirel. Networks*, vol. 25, no. 4, pp. 1685–1695, 2019.

[10] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocess. Microsyst.*, vol. 80, no. October, p. 103352, 2021.

[11] S. Destercke, O. Strauss, S. Destercke, O. Strauss, K. Test, and I. Data, "Kolmogorov-Smirnov Test for Interval Data To cite this version : HAL Id : hal-01045013," 2014.

[12] L. Mora-López and J. Mora, "An adaptive algorithm for clustering cumulative probability distribution functions using the Kolmogorov-Smirnov two-sample test," *Expert Syst. Appl.*, vol. 42, no. 8, pp. 4016–4021, 2015.