LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 11(2025)

SECURING WIRELESS SENSOR NETWORKS FOR SMART GOVERNANCE: A DAVIS MEYER ALGORITHM APPROACH AGAINST BLACK HOLE ATTACKS

D.JeyamaniLatha[1*], B.Diwan[2], K.Nirmal Raja[3]

[1]Associate professor, Dept of ECE, Velammal Institute of Technology-601204, Tamil Nadu, India,
[2]Professor, Dept of CSE, St. Joseph's College of Engg. Tamil Nadu,
[3]Principal, ICCS College of Engineering. and Management, Kerala, India

jeyamanilatha@gmail.com[1]
diwandiwan@gmail.com[2]
nirmalkraja07@gmail.com[3]

*Corresponding Author: D.JeyamaniLatha

Received: 12.09.2025 Revised : 9.10.2025 Accepted: 6.11.2025

Abstract: Wireless Sensor Networks (WSNs) are now a crucial part of contemporary digital infrastructure enabling data-driven governance applications environmental sensing and real-time monitoring in a variety of fields including public safety urban management and the execution of environmental policies. WSNs are vulnerable to various security threats that jeopardize data integrity confidentiality and overall network reliability due to their inherent limitations which include limited energy computational capacity and susceptibility to environmental adversities. Among these the Black Hole attack is a crucial denial-of-service (DoS) vulnerability in which malevolent nodes promote themselves as having the quickest and most recent route to the destination drawing substantial amounts of network traffic. These compromised nodes disrupt data transmission and impair network performance by dropping packets rather than forwarding them after the traffic is rerouted. In order to overcome this difficulty this study presents the Davis Meyer algorithm a reliable cryptographic and routing control system intended to identify and lessen Black Hole attacks in WSN settings. The suggested model increases data transmission reliability reduces packet loss and maintains network lifetime without placing a heavy computational burden on sensor nodes. In addition to strengthening WSNs resistance to malevolent intrusions the suggested method advances the creation of safe sustainable and governance-aligned sensor networks that are appropriate for widespread implementation in smart cities and environmental monitoring systems.

Key Words: Black hole Attack, Davies-Meyer algorithm, Packet loss, Throughput, Trust level, FAR (False Alarm Rate) and MDR (Missed Detection Rate).

1. Introduction:

A Wireless Sensor Network (WSN) is made up of many tiny self-configured devices called sensor nodes that are placed strategically throughout different areas where human access may be difficult or impossible. Temperature humidity air moisture and electrical signals are among the environmental data that these nodes can detect process and transmit. Military surveillance industrial control target tracking home automation space exploration pollution monitoring environmental and earth sensing forest fire and landslide detection healthcare systems area monitoring water quality management and smart grids are just a few of the numerous fields in which WSNs have found widespread use. However sensor nodes are extremely susceptible to security threats and malevolent intrusions due to their inherent limitations which include limited storage capacity limited computational power and energy limitations. As a result a variety of attacks such as wormhole sinkhole selective forwarding Sybil and Black Hole attacks can target WSNs.

An especially dangerous threat is a Black Hole attack in which certain network nodes absorb or discard incoming and outgoing traffic without alerting the source nodes. As a result data packets are silently lost and the source nodes are not aware that their transmissions have not reached their intended destinations. Monitoring and examining the patterns of lost network traffic is usually necessary to identify such attacks [1].

The increasing dependence of smart governance systems and local administrations on wireless sensor infrastructures for tasks like environmental monitoring public safety and digital service delivery has made ensuring secure and reliable data transmission an essential priority [2]. Network performance and the dependability of data-driven decision-making processes in governance frameworks are both at risk from routing-based attacks particularly the Black Hole attack (Figure 1) [3] . The current study aims to identify and

reduce malicious routing behavior in WSNs by presenting an enhanced security mechanism based on the Davis Meyer algorithm [4]. The proposed method achieves resilience against denial-of-service attacks and energy efficiency by combining adaptive routing control with lightweight cryptographic verification . By doing this the research advances the development of a safe and sustainable WSN architecture that is in line with the concepts of smart governance and supports transparent efficient and trustworthy local-level data ecosystems [5].

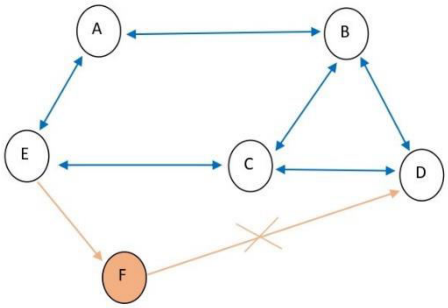

Figure1:Black hole Attack

Wireless Sensor Networks (WSN) use wireless communication to transmit data and are made up of sensor nodes gateways and related software. WSN consists of gateway nodes that route the data and generic nodes that sense it. WSN applications now cover a broad range of electronics such as body sensor networks and smart appliances as IoT has evolved into the Internet of Everything (IoET) [6].

However because of its limited resources WSN is vulnerable to a variety of Denial-of-Service (DoS) attacks including Blackhole Grayhole and Flooding attacks. This paper uses the Low Energy Aware Cluster Hierarchy (LEACH) protocol for experiments and presents a dataset designed specifically for WSN DoS attacks in order to address these vulnerabilities. This dataset is trained using an Artificial Neural Network which achieves high classification rates by classifying different kinds of DoS attacks. The suggested method seeks to lower false alarms and improve attack prevention accuracy [7].

In addition groups of mobile devices that create transient networks—often without a fixed infrastructure—are what define Mobile Ad hoc Networks (MANET) [8]. These networks have dynamic topologies and are susceptible to security breaches especially the Blackhole attack in which malevolent nodes deceive data routing in order to intercept packets [9]. This study investigates the Blackhole attacks effects on network performance in the context of the Ad-hoc On-Demand Vector (AODV) routing protocol [10].

In order to counter this the authors suggest an effective detection method that considerably reduces communication expenses while preserving higher security than current approaches [11]. Additionally by using hop count and creative detection techniques this study presents a lightweight technique for identifying both single and cooperative Blackhole attacks [12]. The suggested techniques outperform standard AODV in terms of improving MANET communications security and dependability [13].

2. Proposed Method:

Malicious nodes are separated using the Davis Meyer algorithm to prevent packet loss during transmission between the source and destination nodes. The suggested algorithms sequential steps are described in the flowchart as shown in Figure 2.

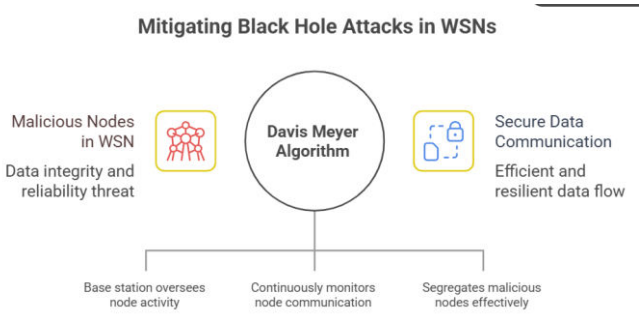

Figure- 2: Flow chart

The system designates a cluster head as the base station where the Davis Meyer algorithm is used in order to track node activity and routing behavior. Using an algorithm that continuously monitors communication patterns and node status regular nodes in this configuration communicate with the base station.

Davies Meyer Algorithm:

Hash function:

$Pr[h \xleftarrow{s} H: h(x) \oplus h(x') = y)] \leq \epsilon$

family of hash function $H = \{h: x \rightarrow y\}$

Distinguishers

$\Delta_D\ (O;P) = P_r\ [D^{\circ} \Rightarrow 1] - P_r\ [D^{p} \Rightarrow 1]$

D ⟶ Distinguisher

Encryption:

Let $\delta, \epsilon \in [0,1]$

$P_r[X_p \in T_{bad}] \leq \delta$

for all $T \in T_{good}$ $\frac{P_r[X_0 = T]}{P_r[X_p = T]} \geq 1 - \epsilon$

[attainable transcripts]

Pseudo random Security:

$Adv^{prf}_{F^{P1,P2}}(D) = \Delta_D[F^{P1,P2}; f]$

Decryption Security:

$Adv^{Prf}_{EDM^{P1,P2}}(D) \leq \frac{q}{2^n} + \frac{(\epsilon^q + 1)}{2^{n\epsilon}}$

Attainable Mappings-Authenticated data packets

$P_{a1} \oplus P_{b1} = x_1,$

$P_{a2} \oplus P_{b2} = x_2,$

$P_{aq} \oplus P_{bq} = x_q$

Towards Secured Data Collection

$P(x) = x', P(P(x)) = P(x') = y \oplus x',$

$P(P(x')) = y' \oplus y \oplus x'$

During the path-finding process the algorithm distinguishes between normal and malicious nodes. Normal nodes only report valid paths whereas malicious nodes promote false routes as the best ways to draw data packets. Because of this clever classification and control malicious nodes are isolated and data packets are safely routed toward the destination instead of being intercepted or dropped in the middle of transmission. In addition to enhancing network trustworthiness and preventing the Black Hole attack this approach guarantees secure efficient and resilient data communication—a critical element of smart governance infrastructures.
The purpose of Davies Meyer Algorithm is to identify malicious nodes and to safeguard the packets to be lost because of not forwarding them. The implementation of Davies Meyer Algorithm is to secure the packet drop and improve the system performance.

2.1 Scenario:

Using the Davis Meyer algorithm an improved Trust Detection model is shown in Figure 3 of the paper. The network simulator NS2 which has a configuration of 100 randomly placed mobile nodes in a field measuring 1000 X 1000 m² is used to assess the models performance. It is estimated that between 10 and 50 percent of the 100 sensor nodes in this network act maliciously by dropping transmitted packets at rates between 50 and 80 percent. Using a Constant Bit Rate (CBR) traffic model packets are sent at a fixed rate of four packets per second assuming a one-minute pause time for each destination node. Table 1 shows the simulations environmental settings.

Table 1.Network configuration parameters.

Sl. No.	Description	Simulation Parameter details for Davis Meyer Algorithm	Simulation Parameter details for FFS Algorithm
1	Area	1000 X 1000 m^2	1000 X 1000 m^2
2	Nodes	100	100
3	Transmission Protocol	UDP	UDP
4	Packet Size	512 bytes	512 bytes
5	Antenna	Omni directional Antenna	Omni directional Antenna
6	Simulation Time	100 Sec	100 Sec
7	Application Traffic	CBR	CBR
8	Initial Energy	0.3J	0.3J
9	Transmitting power	0.15mw	0.15mw
10	Receiving power	0.15mw	0.15mw
11	Routing Protocol	AODV	AODV
12	Que Type	Drop tail	Drop tail
13	Type of Attack	Black Hole Attack	Black Hole Attack
14	Algorithm	Davis Meyer algorithm	FFS Algorithm
15	Propagation	Two Ray Ground	Two Ray Ground

3. Results & Discussion:

3.1Packet loss : Packet loss in wireless sensor network is nothing but the amount of data sent reduces the amount of data received.

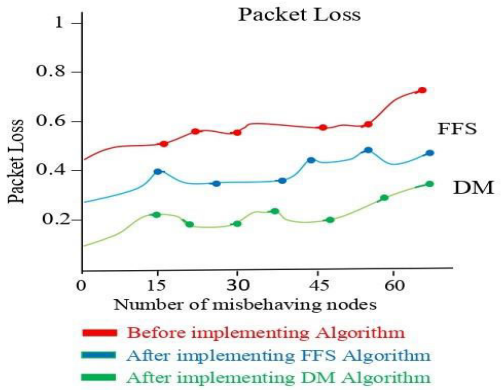

Figure 3:Packet Loss

Figure 3 displays the packet loss results in a wireless sensor network with varying percentages of malicious sensor nodes. Due to black hole attack, the malicious node got the packets from source node and drop it instead of forwarding to the target node.

3.2Energy consumption

By identifying the malicious node as shown in figure 4, the Davies Meyer algorithm overcomes packet loss and improves energy consumption.

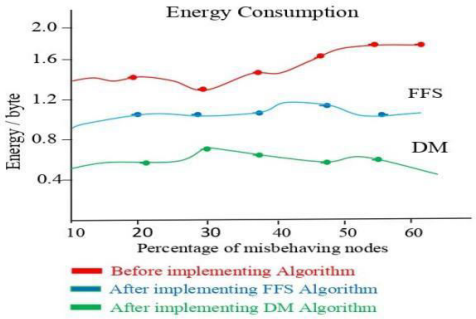

Figure 4:Energy Consumption

3.3 Throughput:

Throughput is defined as the total number of packets transmitted to the specified destination in given time. This metric is high when connectivity and coverage are high in the network. This statistic also assesses the routing algorithm's performance.

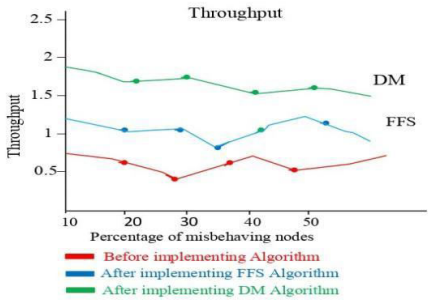

Figure 5: Throughput

As the graph illustrates, the black hole attack randomly reduces the wireless sensor network's throughput because the packet delivery ratio is not as high as anticipated. To improve this, we suggest the Davies Meyer Algorithm, which will identify the malicious nodes from the route in order to eliminate packet drop and significantly increase throughput, as shown in figure 5.

Trust Level:

Trust is the level of belief that is dependent on the entity's accomplishments and only applies within a particular viewpoint at a particular moment, rather than being a fixed value associated with the entity.

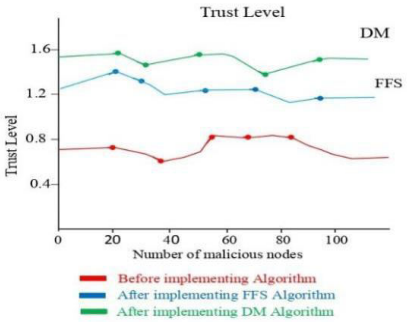

Figure 6: Trust Level

The suggested system uses two metrics—Missed Detection Rate (MDR) and False Acceptance Rate (FAR), which are provided in the following equations—to assess the identification of messages.

$$MDR = \frac{N_{mis}}{N}$$

$$FAR = \frac{N_f}{N_i}$$

where N_f is the number of false recognized by the method, which is recognized as true packets, Ni is the number of packets recognized by the method and N_{mis} is the Number of true packets recognized by the method.

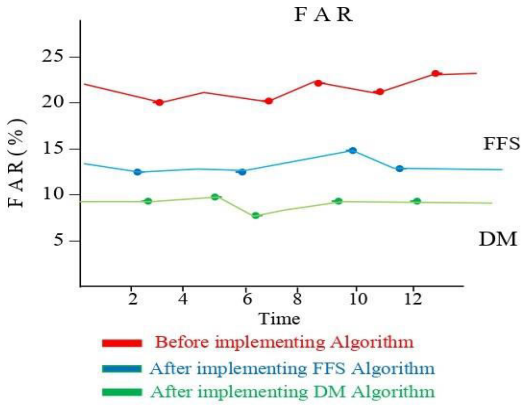

Figure 6: False Acceptance Rate

Due to black hole attack, source node accepting wrong paths as right paths and send the packets. By means of Davies Meyer Algorithm this FAR can be reduced as malicious nodes are detected and packets are routed to the destination instead of dropped and is depicted in figure 6.

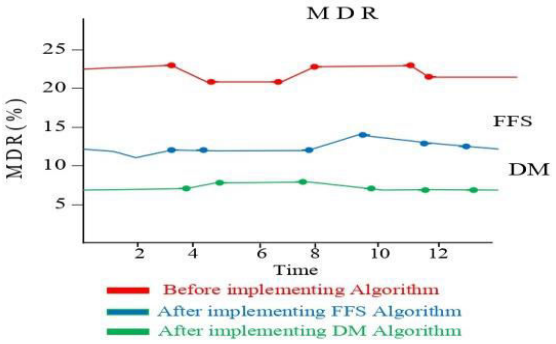

Figure 7: Missed Detection Rate

Because of using Davies Meyer Algorithm, the malicious nodes are detected and the packets' missed rate is also significantly reduced as shown in the Figure 7.

4.Conclusion:

The study shows that the performance and dependability of Wireless Sensor Networks (WSNs) are greatly improved by successfully addressing routing-based threats especially the Black Hole attack. By successfully identifying and isolating malicious nodes using the Davis Meyer algorithm the suggested framework protects network stability and data forwarding. NS2 tool-based simulations show significant gains in a number of performance metrics most notably higher throughput combined with lower packet loss and energy usage suggesting more secure data transfer. Additionally assessments of other metrics like Trust Level False

Acceptance Rate (FAR) and Missed Detection Rate (MDR) validate the algorithms ability to strengthen the networks reliability and resilience.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. All expenses were covered by the authors' affiliated institutions.

Acknowledgments

The authors would like to thank their respective universities and research centers for providing access to library resources and computational facilities. Special appreciation goes to colleagues in the Natural Language Processing and Data Science communities whose constructive feedback during early manuscript discussions helped shape the final review. The authors are also grateful to the anonymous reviewers for their insightful comments and suggestions.

Conflict of Interest

The authors declare that they have no known financial or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES:

1. Ali, S., Khan, M.A., Ahmad, J., Malik, A.W., & ur Rehman, A. (2018). Detection and prevention of Black Hole attacks in IoT and WSN. *Proceedings of the Third International Conference on Fog and Mobile Edge Computing (FMEC)*, 110–115. https://doi.org/10.1109/fmec.2018.8364068
2. Hussain, M., Ren, J., & Akram, A. (2020). Classification of DoS attacks in wireless sensor networks with artificial neural networks. *International Journal of Network Security, 22*(3), 542–549.
3. Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. *Procedia Computer Science, 79*, 715–721. https://doi.org/10.1016/j.procs.2016.03.091
4. Arora, K., Kavita, K., & Jain, V. (2020). Impacts of Black Hole attack on mobile ad-hoc networks. *International Journal of Future Generation Communication and Networking, 13*(4), 644–653.
5. Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of Black Hole attack in mobile ad hoc network. *Proceedings of the International Conference on Intelligent Computing, Communication and Convergence (ICCC)*, 110–115.
6. Jain, R., & Pachouri, R. (2020). Detecting and isolating Black Hole attacks in MANET using counter-based trolling technique. *International Journal of Advanced Research in Computer Science, 11*(6), 50–56.
7. Rani, B., Sehrawat, H., & Siwach, V. (2020). Black Hole attack in wireless sensor network (WSN) using AODV protocol. *International Journal of Advanced Science and Technology, 29*(4), 349–359.
8. Saputra, R., Andika, J., & Alaydrus, M. (2020). Detection of Black Hole attack in wireless sensor network using enhanced check agent. *Proceedings of the Fifth International Conference on Informatics and Computing (ICIC)*, 1–5. https://doi.org/10.1109/icic50835.2020.928857
9. Alattas, R. (2016). Detecting Black Hole attacks in WSNs using multiple base stations and check agents. *Proceedings of the Future Technologies Conference (FTC)*, 1–6. https://doi.org/10.1109/ftc.2016.7821728
10. Dilware, R., Rai, D.K., & Upadhyay, A. (2020). A review on suspicious attack detection. *International Journal of Scientific Research & Engineering Trends, 6*(2), 50–55.
11. Fute, E.T., Nangue, A.T., & Tonye, E. (2020). An efficient and secured AODV protocol against Black Hole attacks on wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS), 18*(6), 15–21.
12. Yilmaz, S., & Dener, M. (2024). Security with wireless sensor networks in smart grids: A review. *Symmetry, 16*(10), 1295. https://doi.org/10.3390/sym16101295
13. Nastjuk, I., Trang, S., & Papageorgiou, E.I. (2022). Smart cities and smart governance models for future cities. *Electronic Markets, 32*, 1917–1924. https://doi.org/10.1007/s12525-022-00609-0