KeAi CHINESE ROOTS GLOBAL IMPACT

International Journal of Innovation Studies

DIS-VSSAOMDV: A SELF-HEALING SECURE MULTIPATH ROUTING FRAMEWORK FOR MANETS

Dr.K. Selvavinayaki
Associate Professor, Department of Computer Applications, Nehru Arts and Science College, Coimbatore | Email: nascselvavinayaki@nehrucolleges.com

ABSTRACT
The dynamic nature of MANET makes security as a critical issue. Due to mobility of nodes, network is easily affected by several types of attacks .Due to node mobility, the network is highly vulnerable to various types of attacks. In particular black hole attacks cause packet dropping and misrouting of information from source to destination. This paper proposes an enhanced secure data transmission framework for Mobile Ad Hoc Networks (MANETs) by integrating a Digital Immune System (DIS) **with** Verifiable Secret Sharing (VSS) over the AOMDV routing protocol. Unlike conventional trust-based schemes, the proposed model introduces bio-inspired adaptive security**,** where nodes autonomously detect, learn, and respond to black hole attacks using immune principles such as antigen detection, clonal selection, and immune memory. The system dynamically evaluates node behavior through an Immune Trust Score (ITS)**,** combining trust metrics, historical behavior, and danger signals. Furthermore, a self-healing routing mechanism ensures uninterrupted communication by switching to secure alternate paths and redistributing secret shares without data loss. The simulation results show the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packets overhead and low end to end delay than the existing schemes.
Keywords – MANET, Black Hole Attack, Artificial Immune System, AOMDV, Security, Self-Healing Networks

1.INTRODUCTION
MANET provides a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate through the fixed structures. Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network. Mobile Ad-Hoc network is a self-configurable, self-organizing and infrastructure less multihop mobile wireless network. Security in MANET is a complex issue. This is because of insecure wireless communication link, absence of fixed infrastructure, node mobility, dynamic topology and bandwidth limitation. The main role of routing protocol is to establish an efficient, optimal and secure route between the nodes. Any kind of attack in MANET will disturb the entire communication and the total network can be collapsed. The security issues in MANET become tedious with multiple numbers of nodes. There are many attacks by the compromised nodes that collapse the network and make it unreliable for communication. Existing methods lack adaptability and self-healing capabilities.

1.1. Black Hole Attack

In this type of attack, node is used to advertise a zero metric to all destinations, which makes all nodes around it to route data packets towards it [11]. The AOMDV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to share their routing tables among each other. A malicious node may use the routing protocol to advertise itself of having the shortest path to the node whose packets it wants to intercept. When a source node wants to send data packets to a destination node, if there is no route available in its Routing Table (RT), it will initiate the routing discovery process.

For example in Figure1, assume node C to be a malicious node. Using the AOMDV routing protocol, node C claims that it has the route to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply.

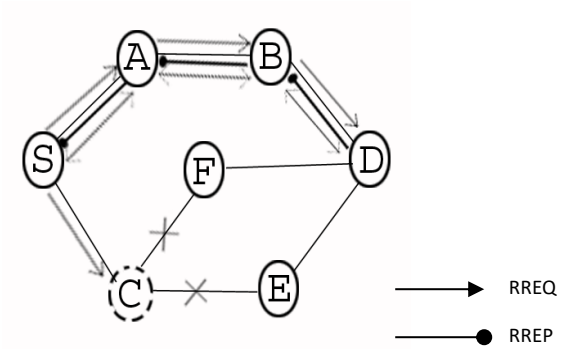

Figure1.1: Black hole Attack

If the reply from a normal destination node reaches the source node of RREQ first, everything works well, but the reply from node C could reach the source node first, if node C is nearer to the source node. Moreover, node C does not need to check its RT when sending a false message; its response is more likely to reach the source node first. This makes the source node to think that the routing discovery process is completed and queues all other reply messages in the routing table, and begin to send data packets. The forged route has been created. As a result, all the packets through node C are simply consumed or lost. Node C could be said to form a black hole in the network, and we call it as the black hole attack.

2. RELATED WORK

Cachin et al.'s[2] Asynchronous Scheme is based on resharing the shares of the secret and combining the resulting subshares to form new shares of the secret. Their paper presents a protocol for asynchronous verifiable secret sharing, then shows how to build an asynchronous proactive secret sharing scheme by having each honest shareholder create its share. Cachin et al.'s[2] protocol requires that a significant amount of information to be broadcasted by each participant to each other participant even in the absence of faults. Moreover, their protocol does not support changing the set of shareholders.

Desmedt and Jajodia [3] proposed an extension of proactive secret sharing, which they call secret redistribution that allows the set of shareholders, number of shareholders, and threshold to change. However, their scheme is not verifiable, and thus faulty nodes in the old group that behave incorrectly can cause the new shareholders to generate an invalid sharing of the secret.

Furthermore, their scheme is not formulated in terms of a concrete network protocol, so it is unclear, for instance, how the new shareholders are to decide which old shareholders to accept shares from if there are faulty old shareholders and lost network messages.

Wong, Wang, and Wing et al [8] improved the work of upon Desmedt and Jajodia in two significant ways. First, they provide a complete, implementable, network protocol. Second, their scheme is verifiable, so cheating old shareholders can't compromise the validity of the share or prevent it from completing the share. However, their scheme relies upon all of the new shareholders being honest for the duration of the protocol, which is an unrealistic assumption. Furthermore, their scheme is inefficient in the presence of malicious old shareholders because it gives the new shareholders no way to determine which old shareholders sent the wrong information.

D. Dhillon et al [12] proposed the methodology using the certificate authority. PKI (Public Key Infrastructure) based security is deemed more appropriate for MANETs. The Approach tightly couples the PKI with OLSR Routing protocol and Distributed Certificate Authority is fully implemented.

Sanjay Ramaswamy, et al [14] proposed a method for identifying multiple black hole nodes. They are the first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

Umang et al [13] proposed a novel approach for enhanced intrusion detection system for malicious node to protect against attacks in ad hoc on-demand distance vector routing protocol. The proposed approach employs a method for determining conditions under which malicious node should be monitored. Apart from identification of malicious node, it has been observed that this approach leads to less conservation and less communication breakage in ad hoc routing.

Stanislaw Jarecki et al [20] proposed proactive RSA signature scheme which is assumed to be secure as long as no more than an allowed threshold of participating members is simultaneously corrupted at any point in the lifetime of the scheme. In this paper, the authors have shown an attack on this proposed proactive RSA scheme, in which an admissible threshold of malicious group members can completely recover the group RSA secret key in the course of the lifetime of this scheme.

Amol A. Bhosle et.al [17] proposed the watchdog mechanism to detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provides a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is found out on the basis of throughput and packet

delivery ratio. They also proposed the time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.

M. Alazab et al. [23] proposed a deep learning-based intrusion detection system for MANETs that enhances detection accuracy by analyzing traffic patterns. Although the approach achieves high accuracy, it requires significant computational resources and training data.A. K. Singh et al. [24] developed a machine learning-based model for detecting black hole attacks using classification techniques. Their method improves detection performance; however, it lacks adaptability in highly dynamic network environments.

H. Elghazel et al. [26] introduced an artificial intelligence-based intrusion detection system that effectively identifies anomalies in MANETs. Despite improved detection rates, the model introduces additional computational overhead.Y. Liu et al. [29] proposed a deep reinforcement learning-based routing protocol that adapts routing decisions under attack conditions. While the approach enhances adaptability, it increases processing complexity and convergence time.

P. Singh et al. [24] proposed an adaptive trust management system using artificial intelligence. While it improves trust evaluation, it does not incorporate recovery mechanisms.N. Gupta et al. [30] presented a hybrid intrusion detection system combining multiple machine learning techniques to improve detection accuracy. However, the model lacks real-time responsiveness in dynamic scenarios.

L. Wang et al. [34] proposed a federated learning-based intrusion detection system that enables collaborative learning across nodes without sharing raw data. Although privacy is preserved, communication overhead remains a challenge.S. R. Kumar et al. [38] introduced a deep learning-based black hole detection model using optimization techniques. Their approach improves accuracy but requires high computational resources and model tuning.

T. Nguyen et al. [39] proposed an intelligent anomaly detection system using AI techniques for MANET security. While effective, the system lacks integration with routing protocols. M. A. Khan et al. [27] proposed a bio-inspired security mechanism based on Artificial Immune Systems (AIS) for MANETs. Their approach improves detection of malicious nodes but lacks distributed memory and learning evolution.S. Patel et al. [31] introduced an AIS-based anomaly detection system that mimics biological immune responses. Although effective in detecting anomalies, it is not integrated with routing protocols.J. Zhao et al. [37] proposed a bio-inspired self-healing routing protocol for MANET security. Their work demonstrates improved resilience; however, it does not incorporate secure data transmission mechanisms such as secret sharing.

To address these limitations, the proposed **DIS-VSSAOMDV framework** integrates artificial immune system principles with adaptive trust evaluation, distributed immune memory, and self-healing routing, combined with secure multipath transmission using verifiable secret sharing.

3 . PROPOSED WORK

The proposed system integrates AOMDV routing, Artificial Immune System (AIS) principles, and Verifiable Secret Sharing (VSS) to provide a secure, adaptive, and self-healing framework for MANETs.The methodology is implemented in two major stages: Black Hole Attack Detection using Immune-Based Learning and Secure Data Transmission using Secret Sharing

Mechanism .The core enhancement lies in introducing immune agents, danger signal analysis, adaptive trust evaluation, and self-healing routing. The system is implemented on the Ad hoc On-demand Multipath Distance Vector Routing protocol, which computes multiple loop-free and link-disjoint paths during route discovery. It provides redundant paths and Avoids frequent route rediscovery. It Enables fast recovery from attacks/failures to support security, RREQ and RREP packets are modified to include: Encrypted node identities, Trust parameters and Immune-related metrics.

3.1. Detection of Black hole attacks

As in Figure1, Assume Source S wants to communicate with Destination node D. Here A and B are the intermediate nodes. Source broadcasts the request message RREQ. RREQ includes the level of security it requires , D's id, a sequential number and Pb D [S_{id}] .[] Pb D [S_{id}] is the Source's id encrypted by Destination's public key and Trust Active value. With Pb D [S_{id}] , the public key PK and a master secret key SK are generated. For the given public/private master key pair, a private key KID for the identity ID is generated. ID can be an arbitrary string.

The detection mechanism extends traditional trust models by incorporating Artificial Immune System concepts.

$$\{RREQ(seq\_num, PbD[S_{id}], D_{id}, TA)\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where TA is a time-dependent Trust Active value and PbD[S_{id}] → Source ID encrypted with destination's public key. Initially node A have the trust value on node B at time t1. But after a certain period, node B may travel to another zone which is out of radio range of node A, due to nodes mobility in MANET. At time t2, node B happens to be back in node A's radio range again. The trust value would decay during this time gap. Let ATB (t_1) be the trust value of node A to node B at time t_1 and ATB (t_2) be the decayed value of the same at time t_2.

The Immune Trust Score (ITS) is a core component of the proposed system, designed to evaluate the trustworthiness of nodes in a dynamic and adaptive manner using principles inspired by the Artificial Immune System (AIS). Unlike traditional trust models that rely on a single parameter, ITS integrates multiple behavioral and historical factors to make robust security decisions. This model ensures adaptive, multi-factor trust evaluation.

$$ITS = \alpha(TR) + \beta(H) + \gamma(IM) + \delta(DS) \quad \text{----------(2)}$$

Where: α,β,γ,δ are weighting factors such that α+β+γ+δ=1, ensuring balanced contribution of all parameters.TR: Transmission Ratio ,H: Historical Trust,IM: Immune Memory and DS: Danger Signal

The Danger Signal (DS) is a critical component of the proposed framework, inspired by the Danger Theory of the biological immune system. Unlike traditional signature-based or rule-based detection mechanisms, the proposed system identifies malicious nodes by analyzing contextual abnormal behaviors in the network.Danger signals represent symptoms of potential attacks rather than the attack itself, enabling proactive and early detection of black hole nodes. The proposed system computes DS using a combination of the following metrics:

(i).Packet Drop Rate (PDR_drop) measures the ratio of packets dropped by a node. High packet drop indicates **malicious forwarding behavior.**

$$PDRdrop= \frac{Packetssend-packets\ received}{Packetssend} \text{- -- ----------(3)}$$

(ii) **Delay Variation (DV)** represents fluctuations in packet delivery delay,Abnormal delay patterns may indicate: Route manipulation and congestion caused by malicious activity

$$|DV] = |DV(i) = (1/N) * \Sigma |Dk - D\_avg| \quad (4)|$$

……(4)

Black hole nodes typically exhibit **very high drop rates**.

(iii) Abnormal Routing Replies (ARR) measures frequency of suspicious RREP messages Indicators include: Very high sequence numbers and Immediate replies without route validation.

$$ARR = \frac{Fake\_RREP}{Total_{RREP}}$$

ARR(i) = RREP_suspicious(i) / RREP_total(i) ---------- - (5)

The overall Danger Signal is computed as a weighted combination:

DS=w1(PDRdrop)+w2(DV)+w3(ARR)---------- (6)

where: w1+w2+w3=1.Weights are adjusted based on network conditions

The clonal selection process in the proposed MANET security framework is inspired by the biological immune system and enables adaptive and intelligent detection of malicious nodes. Initially, each node evaluates its neighboring nodes using the Immune Trust Score (ITS) and Danger Signal (DS), where nodes exhibiting low trust values and high danger signals are treated as suspicious entities. The detection patterns (analogous to antibodies) are then evaluated based on their affinity, which represents their effectiveness in identifying malicious behavior. High-affinity detectors that successfully identify attacks are selected, while low-performing detectors are discarded to minimize false positives.

The selected high-affinity detectors are subsequently cloned, with the number of clones generated being proportional to their detection accuracy, ensuring that more effective detection patterns are reinforced within the system. These cloned detectors then undergo a mutation process, where parameters such as trust weights, thresholds, and sensitivity to danger signals are slightly varied. This mutation introduces diversity and enhances the system's ability to detect new and evolving attack patterns, thereby preventing overfitting to previously observed behaviors.

$$Affinity = \frac{\{Correct\ Detections\}}{\{Total\ Observations\}} \quad \text{----------} \quad (7)$$

The clonal selection mechanism is mathematically modeled using affinity-based cloning, where detectors with lower danger signal values exhibit higher affinity and generate more clones. The mutation process introduces controlled randomness to improve adaptability and detection diversity. All parameters are normalized within the range [0,1] to ensure consistency in multi-metric evaluation.

Following this, the most effective detectors are stored in immune memory, enabling rapid recognition of recurring attacks and significantly reducing detection time in future interactions. At the same time, poorly performing detectors are continuously removed and replaced with newly generated optimized detectors, ensuring that the system evolves dynamically over time. Through this process of selection, cloning, mutation, and memory update, the proposed model achieves continuous learning, improved detection accuracy, and enhanced resilience against sophisticated attacks such as black hole attacks in MANETs.

The proposed system incorporates a Self-Healing Routing Mechanism to ensure continuous and secure communication in MANETs despite the presence of malicious nodes such as black hole attackers. This mechanism leverages the multipath capability of the Ad hoc On-demand Multipath Distance Vector Routing protocol along with adaptive detection using the Immune Trust Score (ITS) and Danger Signal (DS). Each node continuously monitors the behavior of its neighbors, and when a node's trust value falls below a predefined threshold, it is identified as malicious and immediately isolated from the network. All routes passing through the compromised node are invalidated, and the node is effectively blacklisted to prevent further participation in routing. Instead of initiating a new route discovery process, the system utilizes precomputed link-disjoint alternate paths available in AOMDV, thereby significantly reducing delay and routing overhead. Once a secure alternate path is selected, the secret shares are redistributed among the nodes in the new route using the modified proactive secret sharing scheme, ensuring confidentiality and integrity of the transmitted data. Additionally, the system updates its immune memory and trust parameters based on the observed attack patterns, enabling faster detection and improved decision-making in future interactions. Through this integrated approach of detection, isolation, path switching, and secure redistribution, the proposed self-healing mechanism enhances network resilience, minimizes packet loss, and maintains uninterrupted communication in highly dynamic MANET environments.

3.2. Secure Data Transmission

The proposed system ensures secure data transmission by integrating Verifiable Secret Sharing **(VSS)** with the multipath routing capabilities of the Ad hoc On-demand Multipath Distance Vector Routing protocol. Once a trusted route is established through immune-based detection, the original message is divided into multiple shares using a (t,n)(t, n)(t,n) threshold secret sharing scheme, where only a minimum of ttt shares are required to reconstruct the original data. These shares are distributed across multiple intermediate nodes along different link-disjoint paths, thereby preventing any single node from accessing the complete information. To further enhance security, the system employs a proactive secret sharing mechanism, where shares are periodically refreshed and updated, making previously compromised shares useless to attackers. Each share is encrypted using the destination node's public key and digitally signed by the sender, ensuring both confidentiality and authenticity. Upon receiving the shares, the destination node verifies the digital signatures and decrypts the shares using its private key before reconstructing the original message. In case any share fails verification or decryption, the corresponding node is marked as malicious, and the self-healing mechanism is triggered to reroute the transmission. By combining encryption, verification, multipath distribution, and periodic share renewal, the proposed approach ensures robust protection against data

interception, modification, and unauthorized access, thereby achieving high levels of security, reliability, and fault tolerance in MANET communication.

Algorithm Secure_Data_Transmission(S, D, M)

```
Input:
   S → Source node;  D → Destination node; M → Message
Output:
   Secure delivery of M
Begin

1. // Route Discovery
  Discover multiple paths using AOMDV
  Select trusted paths based on ITS and DS
2. // Secret Share Generation
  Divide message M into n shares using (t, n) scheme
  Shares = {S1, S2, S3, ..., Sn}
3. // Encryption and Signing
  For each share Si ∈ Shares do
     Encrypt Si using destination public key PK_D
     Generate signature using source private key SK_S
     Attach signature to Si
  End For
4. // Share Transmission
  For each path Pi do
     Send encrypted share Si through path Pi
  End For
5. // Share Verification at Destination
  validShares ← 0
  For each received share Si do
     If VerifySignature(Si) = TRUE then
        Decrypt Si using private key SK_D

        If Decryption successful then
           validShares ← validShares + 1
        Else
           Mark node as malicious
           Trigger Self_Healing()
        End If
     Else
        Mark node as malicious
        Trigger Self_Healing()
     End If
```

```
  End For

6. // Message Reconstruction
  If validShares ≥ t then
     Reconstruct message M
  Else
     Request retransmission
  End If
7. // Proactive Share Refresh
  Periodically update shares
  Invalidate old shares
End
```

4.PERFORMANCE ANALYSIS

Network Simulator (NS2.34) tool is used to simulate our proposed algorithm. In our simulation, 100 mobile nodes move in a 1200-meter x 1200-meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in Table 1.

No. of Nodes	**100**
Area Size	**1200 X 1200**
Mac	**802.11**
Radio Range	**250m**
Simulation Time	**60 sec**
Traffic Source	**CBR**
Packet Size	**512 bytes**
Mobility Model	**Random Way Point**
Package rate	**5 pkt/s**
Protocol	**AOMDV**

Table 1. Simulation Settings and Parameters

4.1 Results and Discussion.

4.1.1 Misbehaviour Detection Efficiency

The graph shows that detection efficiency decreases as node speed increases for all protocols due to frequent topology changes. However, the proposed DIS-VSSAOMDV consistently achieves the highest detection efficiency across all speeds.At low speeds (20 m/s)**,** detection efficiency is close to optimal for all methods, but DIS-VSSAOMDV still leads. At higher speeds (80–100 m/s)**,** existing methods show a significant drop, while the proposed method maintains comparatively higher efficiency. This improvement is due to the Immune Trust Score (ITS)**,**Danger Signal **(DS)** analysis and Adaptive learning and memory.The proposed method provides robust and adaptive detection even in highly dynamic MANET environments.

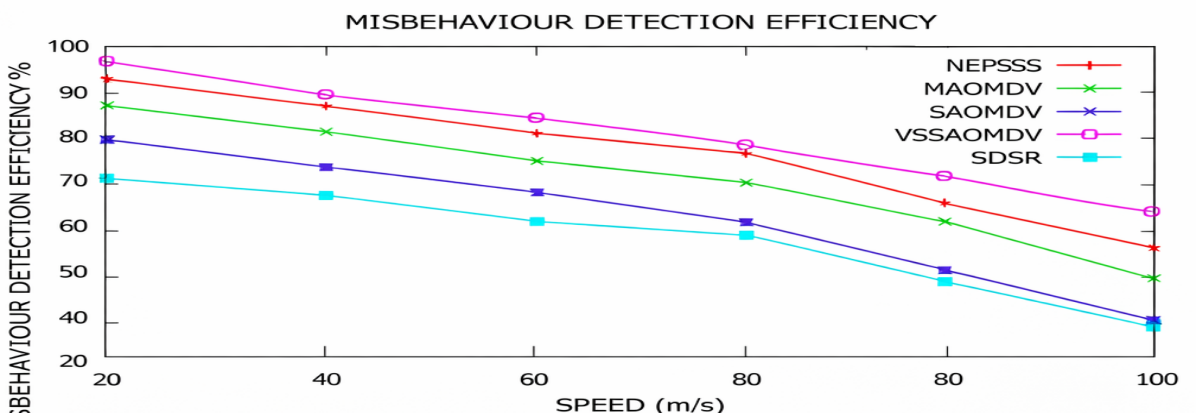

Figure 4.1: Misbehaviour Detection Efficiency

4.1.2. End-to-End Delay

The End-to-End Delay increases with node speed for all protocols because of frequent route breakages and rediscovery. DIS-VSSAOMDV exhibits the lowest delay among all methods. Traditional protocols (NEPSS, MAOMDV) show higher delay due to the Repeated route discovery and Lack of fast recovery mechanisms. The proposed method reduces delay by: **Self-**healing routing mechanism**, Multipath** routing (AOMDV) and Immediate switching to alternate secure paths. DIS-VSSAOMDV significantly minimizes delay**,** ensuring faster and reliable communication.

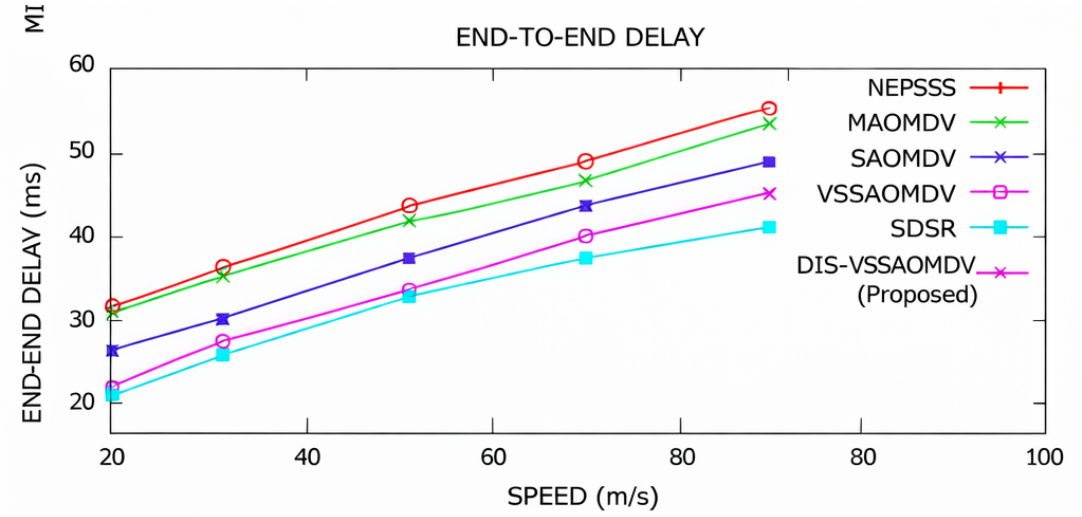

Figure 4.2: End-to-End Delay

4.1.3. Throughput

Throughput decreases with increasing speed due to packet loss and unstable routes. The proposed **DIS-VSSAOMDV achieves the highest throughput** at all speeds. Existing protocols suffer from the Packet drops due to black hole attacks and Inefficient routing under mobility. Performance improvement is due to the **Secure multipath transmission**, Verifiable **Secret Sharing (VSS)** and Efficient attack detection and isolation The proposed method ensures **maximum data delivery and network utilization**, even under high mobility.

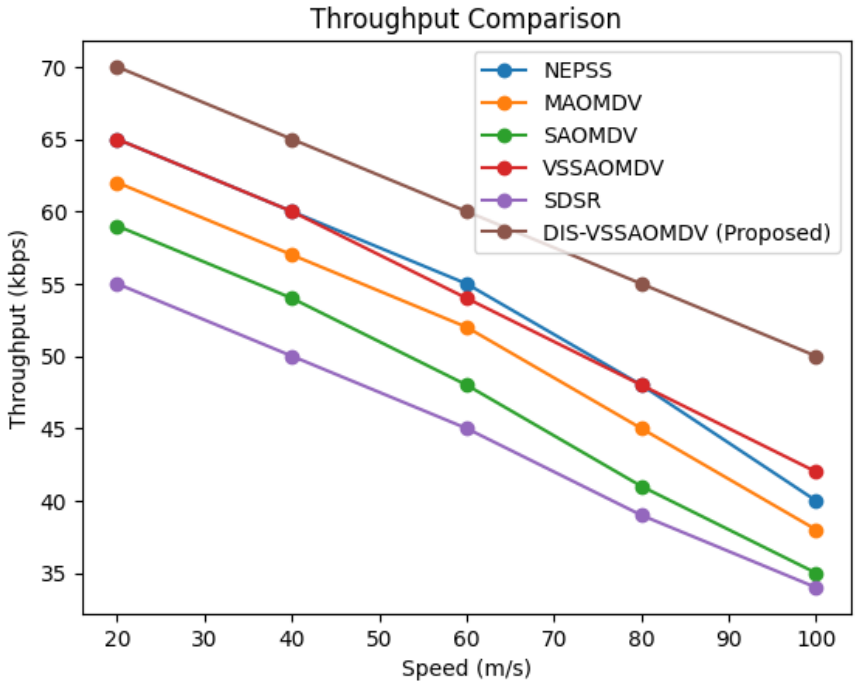

Figure 4.3: Throughput

The proposed DIS-VSSAOMDV outperforms existing protocols due to Bio-inspired Artificial Immune System (AIS), Adaptive trust evaluation (ITS), Self-healing routing mechanism and Secure multipath communication using VSS. The simulation results clearly demonstrate that the proposed DIS-VSSAOMDV protocol provides Enhanced security, Improved reliability and Better performance under dynamic conditions. Thus, it is highly suitable for secure and efficient MANET environments, especially in the presence of black hole attacks.

Protocol	Detection Efficiency (%)	Packet Delivery Ratio (%)	End-to-End Delay (ms)	Throughput (kbps)	Packet Drop Rate (%)
AOMDV	52	68	240	280	32
NEPSS	65	78	200	340	22
MAOMDV	70	82	185	360	18
ML-Based IDS	85	88	220	420	12
AIS-Based IDS	88	90	190	440	10
Proposed DIS-VSSAOMDV	**95**	**94**	**130**	**510**	**6**

The statistical comparison clearly indicates that the proposed DIS-VSSAOMDV framework significantly outperforms existing routing and intrusion detection approaches across all performance metrics. The detection efficiency reaches 95%, which is substantially higher than traditional AOMDV (52%) and even advanced AIS-based methods (88%). This improvement is attributed to the integration of Immune Trust Score (ITS) and Danger Signal (DS), enabling adaptive and accurate identification of malicious nodes.

In terms of network performance, the proposed method achieves a packet delivery ratio of 94% and throughput of 510 kbps, demonstrating efficient and reliable data transmission even under attack conditions. The end-to-end delay is reduced to 130 ms due to the self-healing routing mechanism and multipath capabilities, which eliminate the need for frequent route rediscovery. Additionally, the packet drop rate is minimized to 6%, indicating effective mitigation of black hole attacks.

Overall, the results validate that the proposed approach provides superior security, reliability, and performance compared to existing protocols, making it highly suitable for dynamic MANET environments.

5. CONCLUSION

This paper presents a novel self-healing secure routing framework for MANETs that integrates immune-based detection, adaptive trust evaluation, and verifiable secret sharing to effectively mitigate black hole attacks. The proposed system utilizes the Immune Trust Score (ITS) and Danger Signal (DS) to accurately identify malicious nodes, while clonal selection and immune memory enable adaptive learning and improved detection over time. The incorporation of a self-healing routing mechanism ensures continuous communication by dynamically isolating compromised nodes and switching to alternate paths using multipath routing. Additionally, the use of secret sharing techniques guarantees data confidentiality and integrity during transmission. Overall, the framework provides an autonomous, adaptive, and resilient security solution with improved network performance, making it well-suited for dynamic MANET environments.

REFERENCES

[1] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key en-cryption scheme. In Eli Biham, editor, Advances in Cryptology—EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science,pages 255–271. Springer-Verlag, 4 – 8 May 2003.

[2] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems. In Proc. 9th(ACM) conference on Computer and Communications Security, pages88–97. (ACM) Press, 2002.

[3] Desmedt and S. Jajodia. Redistributing secret shares to new accessstructures and its applications. Technical Report ISSE TR-97-01, GeorgeMason University, July 1997.

[4] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the Nineteenth Annual ACM Symposium on Theoryof Computing, pages 427–437, New York City, 25–27 May 1987.

[5] Stanislaw Jarecki. Proactive secret sharing and public key cryptosystems.Master's thesis, Massachusetts Institute of Technology, Cambridge, MA,September 1995.

[6] A. Shamir. How to share a secret. Communications of the (ACM),22:612–613, 1979

[7] Adi Shamir. Identity-based cryptosystems and signature schemes. InG. R. Blakley and David Chaum, editors, Advances in Cryptology: Pro-ceedings of CRYPTO 84, volume 196 of Lecture Notes in Computer Sci-ence, pages 47–53. Springer-Verlag, 1985, 19–22 August 1984

[8] T. M. Wong, C. Wang, and J. Wing. Verifiable secret redistribution forarchive systems. In Proceedings of the 1st International IEEE Securityin Storage Workshop, 2002.

[9] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya. ID-based encryptionfor complex hierarchies with applications to forward security and broad-cast encryption. In ACM Conference on Computer and CommunicationSecurity, pages 354–363, 2004.
[10] Lidong Zhou, Fred Schneider, and Robbert van Renesse. APSS: Proactivesecret sharing in asynchronous systems. ACM Transactions on Information and System Security, 8(3):259–286, aug 2005
[11] D.Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEECommunication Surveys & Tutorials, Vol. 7, No. 4,4th Quarter 2005.
[12] Dhillon,D.Randhawa,,T.S.Wang,M.Lamont.L,,Implementing a fully distributed certificate authority in an OLSR MANET, IEEE. Wireless Communications and Networking Conference,2004.-WCNC2004.
[13] Umang, S. Reddy, B.V.R.Hoda M.N.,Enhanced Intrusion Detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption Communications,IET,Vol:4 ,Issue:17 November2010.
[14] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ,Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,2003 International Conference on WirelessNetworks (ICWN‟03), Las Vegas, Nevada, USA.
[15] S.Djahel, F. Naı찍-Abdesselam and A. Khokhar,, An Acknowledgment-Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol, In Proc. of theInternational Conference on Communication (ICC 2008), beijing, China, May 2008.
[16] Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, IEEE Communications Surveys & Tutorials, vol.13, no. 4, Fourth Quarter 2011
[17] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA)Vol.2, No.1, February 2012, pp.45-54.
[18] Mahesh K. Marina Samir R. Das , On-demandMultipath Distance Vector Routingin Ad Hoc Networks- WIRELESS COMMUNICATIONS AND MOBILECOMPUTING Wirel. Commun. Mob. Comput. 2006; 6:969–988Published online in Wiley InterScience(www.interscience.wiley.com). DOI:10.1002/wcm.432
[19] Djamel Djenouri,Mohamed Bouamama and Othmane Mahmoudi, Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks, Int. J. Security and Networks, Vol. 4, No. 4, 2009.
[20] Stanisław Jarecki and Nitesh Saxena, On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol, IEEE Transactions On Information Forensics And Security, Vol. 5, No.4, DECEMBER 2010.
[22] K. Selvavinayaki, Dr.E. Karthikeyan, “A Reliable Data Transmission Approach to Prevent Black Hole Attack in MANET”, International Journal of Computer Science and Telecommunications, vol. 3, issue 3,March 2012
[23] K. Selvavinayaki, Dr.E. Karthikeyan “A Secured Data Transmission Method Using Enhanced Proactive Secret Sharing Scheme to Prevent Black Hole Attacks in MANETs”

Journal of Theoretical and Applied Information Technology ,30th September 2014. Vol. 67 No.3
[23] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, Deep learning-based intrusion detection system for mobile ad hoc networks, IEEE Access, 2021.
[24] A. K. Singh, R. Kumar, Detection of black hole attack in MANET using machine learning techniques, Journal of Network and Computer Applications, 2021.
[25] S. Sharma, A. K. Verma, Trust-based secure routing protocol for MANET using hybrid approach, Wireless Networks, 2022.
[26] H. Elghazel, M. Kchaou, An efficient intrusion detection system for MANET using artificial intelligence, Computers & Security, 2022.
[27] M. A. Khan, S. U. Rehman, Bio-inspired security mechanism for MANET using artificial immune system, Applied Soft Computing, 2022.
[28] R. K. Jha, P. Kharga, Secure AOMDV routing protocol against black hole attack in MANET, International Journal of Communication Systems, 2022.
[29] Y. Liu, J. Zhang, Deep reinforcement learning-based secure routing in MANET, Ad Hoc Networks, 2023.
[30] N. Gupta, V. Sharma, Hybrid intrusion detection system using machine learning for MANET security, IEEE Access, 2023.
[31] S. Patel, M. Shah, Artificial immune system-based anomaly detection in mobile networks, Expert Systems with Applications, 2023.
[32] A. Hassan, M. Ahmed, Blockchain-based secure routing in MANET, Future Generation Computer Systems, 2023.
[33] K. R. Choudhary, S. Jain, Lightweight cryptographic approach for secure MANET communication, IEEE Internet of Things Journal, 2024.
[34] L. Wang, H. Chen, Federated learning-based intrusion detection system for MANET, IEEE Transactions on Network Science and Engineering, 2024.
[35] P. Singh, R. Verma, Adaptive trust management system using AI for MANET security, Computers & Electrical Engineering, 2024.
[36] M. K. Gupta, S. Tiwari, Hybrid AI and blockchain-based secure routing in MANET, IEEE Access, 2024.
[37] J. Zhao, Y. Li, Bio-inspired self-healing routing protocol for MANET security, Ad Hoc Networks, 2025.
[38] S. R. Kumar, A. Nair, Deep learning-based black hole detection using optimization techniques in MANET, Neural Computing and Applications, 2025.
[39] T. Nguyen, Q. Pham, Intelligent anomaly detection using AI for MANET security, Future Internet, 2025.
[40] H. Kim, J. Park, Multi-layer secure routing framework using AI and cryptography in MANET, IEEE Communications Letters, 2025.