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

STRENGTHENING DATA GOVERNANCE AND NETWORK RELIABILITY IN LOCAL SELF-GOVERNMENT SYSTEMS THROUGH PRIVACY-PRESERVING MULTI-HOP COMMUNICATION FRAMEWORKS

K G Arunkumar[1], G.Singaravel[2]

[1*]Assistant Professor, Department of Computer Science and Engineering
Excel Engineering college (AUTONOMOUS), Komarapalayam-637303
[2]Professor, Department of information Technology,K.S.R.College of Engineering (Autonomous)
Tiruchengode -637215, Namakkal District, Tamilnadu, India

Corresponding Email : arunkumarkg111983@induniversityedu.org[1]

Abstract: This study recontextualizes data integrity and privacy within the domain of local self-government administration, where decentralized communication networks increasingly support governance functions such as e-governance, citizen service delivery, and inter-departmental coordination. The proposed privacy-preserving framework ensures secure data transmission across municipal communication infrastructures employing multi-hop wireless networks. It focuses on detecting malicious packet drops and mitigating link-related disruptions that may compromise transparency and reliability in digital public administration. The framework utilizes a Homomorphic Linear Authenticator (HLA) to enable secure verification of transmitted data without breaching confidentiality, while an external auditing mechanism monitors packet flow integrity to maintain trust and accountability—key tenets of effective local governance. The model's four operational phases—Data Transmission, Verification, Auditing, and Attack Detection—mirror administrative workflows requiring secure data validation and oversight. Simulations conducted under various network loads and governance scenarios demonstrate improved accuracy in detecting intentional data manipulation, reduced false positives, and enhanced reliability in communication infrastructures. By fortifying digital governance networks, this research contributes to more resilient, transparent, and trustworthy local government systems in the era of smart governance.

Keywords: Local Self-Government, E-Governance, Data Integrity, Privacy-Preserving Communication, Homomorphic Linear Authenticator (HLA), Network Accountability, Smart Governance Infrastructure

1. Introduction

The networks primary goal is to share the gathered data with the most influential node and communication is the most crucial function of sensor nodes. Nevertheless direct communication isnt always feasible. It makes sense that intermediate nodes allow the source to reach the destination even though it cannot do so directly. Quickly and unalteredly forwarding the message to the destination is the responsibility of intermediate nodes [1]. Routing refers to the complete process of sending a message from its source to its destination [2]. The most fundamental task performed by any sensor node is routing which also uses the most energy. The lifespan of the sensor network decreases when the sensor nodes use excessive amounts of energy. Reducing the lifespan of the sensor nodes makes it impossible to fully achieve the networks goal [3–4]. In order to maintain the environment a large number of tiny lightweight wireless sensor nodes are deployed in highly dispersed networks known as Wireless Sensor Networks (WSN) [5]. One of the thoroughly studied research fields that is ideal for many real-time applications is WSN [6–8]. Instantaneous communication is necessary in todays fast-paced world and WSN makes it possible. The sensor nodes sense their surroundings and communicate the information they gather to either the sink node or the base station [9–10]. Another name for the sink node is the destination node. It is possible for the sensor node to be a source intermediate cluster sink or destination node [11].

The sensor nodes in WSNs are primarily placed in hostile environments and the network structure is dynamic [12]. Therefore in the event of a system failure accessing the sensor nodes is challenging. In addition WSN does not use a centralized authority to verify that sensor nodes are operating properly. By adhering to better network organization concepts these disadvantages can be addressed [13]. In essence the sensor nodes are arranged either hierarchically or flatly. In the query-based routing technique a node sends a network query to the data-holding node which replies with the data. The language used to present these queries is either high level or simple. According to [14] directed diffusion is among the best instances of query-based routing. The base station sends a message to the whole network using this method. It is assumed that the sensor nodes

forward the data via the path once the data matches the message [15–16]. Even though computer science and information technology are expanding quickly smartphones are becoming more and more popular over time. The goal of ad hoc networking a rapidly expanding field of study is to enable communication between two nodes without the need for a centralized organization [17].

One type of wireless communication network without a fixed infrastructure or static base station is called a mobile ad hoc network (MANET) its topology changes regularly. Wireless networks however can be used with any network topology. E. infrastructure or ad hoc infrastructure-less. Multi-hop communication and peer-to-peer data transmission are supported by the ad hoc topology used by MANET which is a collection of mobile nodes [18]. However quality of service (QoS) varies from network to network and depends on aspects like coverage ratio user mobile device specifications data rate packet size and size [19].

2. Methodology

2.1 Data Collection And Parameters

The Coimbatore Special Economic Zone (SEZ) in Tamil Nadu India (11. 0306° N 77. 0175° E) served as a model for urban local bodies (ULBs) moving toward smart governance and e-administration where data collection for this study was carried out. Data was collected from municipal communication nodes such as data offices citizen service centers and IoT-enabled civic units like water and waste systems. Through a multi-hop wireless governance network running at 500 Mbps traffic volume 200 Mbps link capacity and 0. 5 percent packet loss rate the experiment replicated real-time interdepartmental data exchange. Stable transmissions were ensured by an SNR of 35 dB and latency and jitter of 120 ms and 15 ms respectively. With a congestion window of 20000 bytes and a 256 MB buffer across 50 100 and 150 nodes within a 1000 m² area 15 routing changes and low error rates (0. 002 percent) were simulated to evaluate network resilience.

2.2 .Network Model

This research focused on analyzing the impact of malicious packet drops packet drops due to link errors and the role of an Auditor Ad in network and attack models. Malicious packet drops were deliberate actions by attackers to disrupt communication or degrade service quality while packet drops due to link errors occurred naturally due to poor network conditions such as congestion or faulty hardware. The Auditor Ad acted as a monitoring entity that detected recorded and audited suspicious network activities aiming to differentiate between intentional malicious drops and those resulting from link failures. These components were integrated by the suggested model in Figure 1 to evaluate network security and dependability enabling a strong framework to reduce different attack vectors and maximize overall network performance.

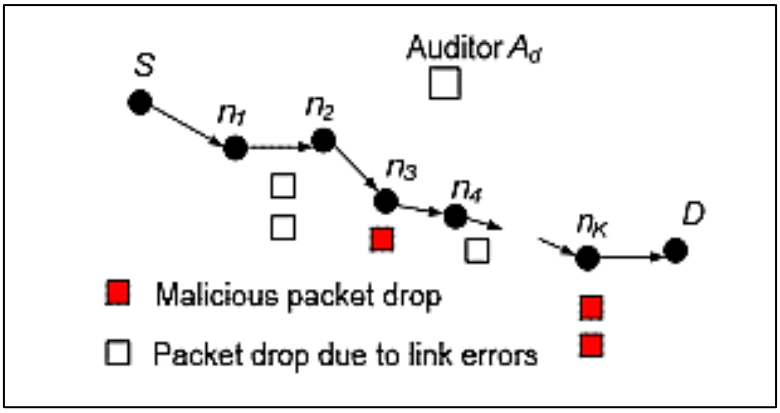

Fig 1 Attack and Network Model

2.3.Proposed architecture

The suggested governance communication architecture enhances data transmission verification auditing and threat detection in municipal multi-hop wireless networks through four operational phases that correspond with administrative workflows. In Phase 1: Data Transmission municipal nodes transmit encrypted governance packets containing a packet-loss bitmap to ensure transmission integrity supported by a Homomorphic Linear Authenticator (HLA) for privacy-preserving validation using cryptographic hash functions and digital signatures. Each node records proof-of-reception in a governance audit database to maintain continuous verification across departmental communications. Phase 3: Auditing and Oversight offers a decentralized auditing protocol based on HLA that confirms packet integrity without revealing private governance data. To boost trust each municipal node generates an encrypted authenticator and the monitoring authority verifies packet-loss bitmaps and identifies anomalous patterns that may indicate breaches.

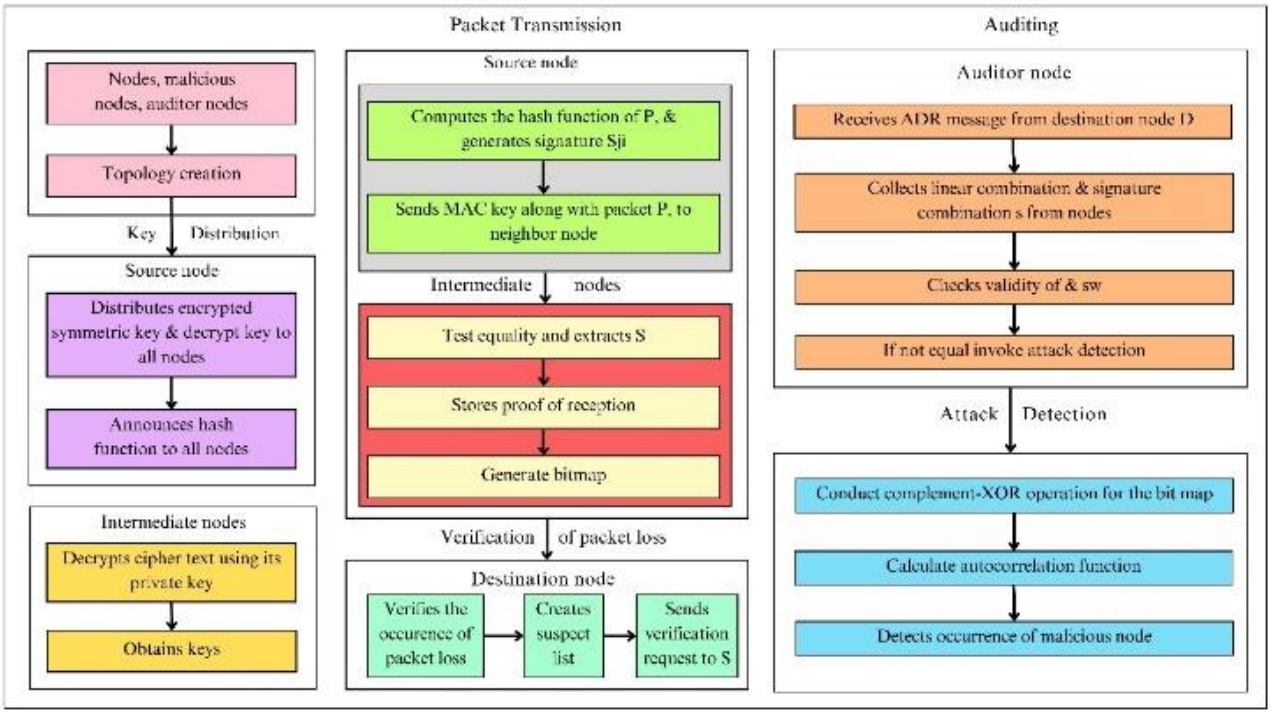

Fig 2 Proposed architecture

In Phase 4: Threat Detection and Accountability Assessment mathematical models assess the risk of malicious interference flagging nodes with persistent irregularities for investigation to support real-time governance monitoring and accountability. Together these stages ensure the dependability and confidence of regional e-governance systems by fostering communication that protects privacy strong data validation and open digital administration.

3.Phase 1

3.1.Packet Transmission

A network node sends packets to its neighboring nodes and the packet-loss bitmap (M) records the status of each packet. Both malicious packet drops and natural channel errors have an impact on the probability of packet loss (P_{loss}), and successful packet transmission ($P_{success}$). The public auditing mechanism that is based on HLA is used to verify packet loss. This is how the auditing process is expressed mathematically in (Eq.1).

$$Verify\ (\mathrm{C}, \mathrm{M}, \mathrm{HLA}) \rightarrow True/False, \quad (1)$$

where HLA and the encrypted packet-loss bitmap denote the linear authenticator signature represented by C. The correlation metrics for determining whether the loss is random, which is caused by natural errors, or correlated that signals malicious activity are calculated using the loss pattern seen in bitmap M.

An indication that the packet loss is suspicious is given if the correlation coefficient is higher than a predetermined threshold α. After the keys are distributed source node S. Pi transmits the packet is the packet that S chooses to send "i " is the sequence number that packets are given to be uniquely identified. Equation 2 illustrates about

$$S_{ji} = \left[H_2(i||j)u^{ri}\right]^x,\ for\ j = 1, \dots, k, \tag{2}$$

Here a one-way chained encryption is used, it prevents an upstream node from deciphering the signature sent to downstream nodes. By using this one-way encryption, the S_{ji} is sent along with Pi. S also iteratively computes the following parameters as in equation 3.

$$\tilde{S}_{Ki} = encrypt_{keyk}(SKK_K),$$
$$T_{Ki} = \tilde{S}_{Ki}||MAC_{keyk}\left(\tilde{S}_{Ki}\right)$$

$$T_{ji} = \tilde{s}_{si}||\ MAC_{kejj}\left(\tilde{s}_j\right) \tag{3}$$

If the test result is true, then n1 decrypts 1i as shown in equation 4.

$$Decrypthey1\left(\tilde{S}_{1i}\right) = S_{1i}||T_{2i}. \tag{4}$$

The loss of P_i is stored in the proof of reception database by n1 if the equality test is unsuccessful. But, n1 saves r_i and s_{1i} in its proof of reception database after the test is shown to be accurate. Following packet reception each node saves the reception data in a database that is kept up to date by each node separately. The information is kept on a FIFO basis. Later auditing uses this proof. Next n_1 transmits a packet containing P_i

and τ_{2i} to n_2. At each intermediate node n_j the aforementioned procedure is repeated. Node nk the final intermediate node only sends Pi to D.

4. Phase 2

4.1 Packet Loss Verification with Proposed Algorithm

A packet loss verification algorithm that can accurately differentiate between packet losses resulting from malicious drops and those caused by natural errors is proposed using packet loss correlation patterns. The primary idea is to analyze the sequence of packet losses over time and look for patterns of correlated losses that are suggestive of malicious activity as opposed to random packet drops caused by link errors. Verification begins with tracking each packet's transmission status over a multi-hop communication path. Information about the packet status for each node is contained in a packet loss bitmap M, a binary array that shows whether each packet was dropped (1), or successfully received (0). By dropping packets 1, 3, and 5 for example the bitmap for this sequence would be M=[0,1,0,1,0]. The proposed algorithm records a sequence of packet losses and then uses a sliding window technique to find the correlation between subsequent packet losses in equation 5.

$$\rho = \frac{\sum_{k=1}^{n}(x_k - \bar{x})(y_k - \bar{y})}{\sqrt{\sum_{k=1}^{n}(x_k - \bar{x})^2 \sum_{k=1}^{n}(y_k - \bar{y})^2}} \tag{5}$$

Where x_k and y_k are the packet loss data for two nodes, $\bar{x}$, and $\bar{y}$ are their respective means. When the computed correlation coefficient ρ for a series of packet losses exceeds a predetermined threshold α, it suggests

that an insider attacker is selectively dropping the packets rather than letting them happen at random. This strongly suggests that the network is being attacked maliciously.

Algorithm: Pseudo code for verification of packet loss

```
Input:
   Packet_Loss_Bitmap[] - Bitmap indicating packet status (1 = lost, 0 = received)
   Threshold - Correlation coefficient threshold
   Sliding_Window_Size - Size of sliding window

Output:
   Suspect_List[] - List of suspicious nodes
   Attack_Detected - Boolean (True/False)

Step 1: Initialize
   Suspect_List = []
   Attack_Detected = False

Step 2: Calculate Correlation for each Sliding Window
   for i = 0 to length(Packet_Loss_Bitmap) - Sliding_Window_Size:
      Window = Packet_Loss_Bitmap[i:i+Sliding_Window_Size]
      Correlation = Calculate_Correlation(Window)
      if Correlation > Threshold:
         Add suspicious node to Suspect_List
         Attack_Detected = True

Step 3: Compare Expected vs Actual Packet Count
   for each node:
      if Count_Received_Packets(node) < Expected_Packet_Count(node):
         Add node to Suspect_List

Step 4: Return Results
   return Suspect_List, Attack_Detected

Function: Calculate_Correlation(Window)
   Return correlation based on statistical method
```

5. Phase 3

5.1 Auditing Method with Homomorphic Linear Authenticator (HLA)

The Homomorphic Linear Authenticator (HLA)-based auditing technique uses a methodical procedure to confirm the veracity of packet loss data reported by nodes in a Multi-Hop Wireless Ad Hoc Network. Each node first computes an authenticator using its private key and creates a packet loss bitmap that represents lost packets. This authenticator is sent to a monitoring node that handles verification together with the encrypted packet loss bitmap. To ensure privacy the monitoring node performs a verification check after receiving the encrypted data using the homomorphic properties of HLA without decrypting the data. And, how each auditing node gets ready for the process. Every node in the path receives a random challenge vector from the auditor node. The received packet's sequence number is kept in the database at every node. Based on this database-stored proof of reception node n_j creates the bit map b_j. In this case j = (bj1…..). b_{ji}=1 indicates that the packet was received at that specific node and b_{ji}=0 indicates that it was not received at that specific node (b_{jM}).

Equations (6) and (7) compute the linear combination $r_{(j)}$ and an extended HLA signature combination $s_{(j)}$ at node n_j.

$$r^{(j)} = \sum_{i=1}^{M} , b_{ji} \neq 0 \text{Cjir}_i \quad (6)$$

$$\mathbf{S}(j) = \prod_{i=1,\, b_{ii}\neq 0} s_{ii}^{c_{ji}} \quad (7)$$

Based on established channel conditions the monitoring node compares the encrypted packet loss bitmap to the anticipated pattern. A node is marked as potentially malicious if anomalies such as departures from the typical packet loss pattern brought on by malicious drops are found.

6.Phase 4

6.1 Attack Detection with Mathematical Formulations

The attack detection algorithm is used after the HLA system has confirmed the packet loss patterns. To ascertain whether the packet loss is the result of malicious drops or link errors this algorithm employs a thresholding technique in conjunction with the correlation analysis from the previous section. The steps for detecting attacks are listed below.

The correlation between the packet losses across different nodes is computed using the equation (8)

$$Correlation\left(x_i, x_j\right) = \frac{\sum_{k=1}^{n} \left(x_i[k] - \overline{x_i}\right)\left(x_j[k] - \overline{x_j}\right)}{\sqrt{\sum_{k=1}^{n} \left(x_i[k] - \overline{x_i}\right)^2 \sum_{k=1}^{n} \left(x_j[k] - \overline{x_j}\right)^2}}, \quad (8)$$

where x_i and x_j are the sequences of packet loss for nodes i and j, and x_i^- and x_j^{--} are their respective means. Following the computation of the correlation coefficients the system compares the results to a predetermined cutoff point α. The event of packet loss is marked as potentially malicious if the correlation coefficient is greater than α. Next the likelihood of finding malicious drops P_{md} is computed using equation (9):

$$P_{md} = \frac{Number\ of\ Malicious\ Detections}{Total\ Number\ of\ Malicious\ Drops} \quad (9)$$

The false alarm rate P_{fa} is an important metric to evaluate the effectiveness of the detection mechanism. It is calculated as equation (10):

$$P_{fa} = \frac{Number\ of\ False\ Alarms}{Total\ Number\ of\ Non-Malicious\ Drops} \quad (10)$$

In this case, P_{fa} is the percentage of harmless packet losses mistakenly labeled as malicious. Indicators of improved detection performance include lower false alarm rates.

6.2 Key Distribution Mechanism

At the network initialization stage, a public-private key pair (K_{pub}, K_{priv}) is assigned to each node. To ensure that each node can securely encrypt and decrypt messages the public keys are transferred between the nodes over a secure channel. Furthermore, the packet-loss bitmaps are encrypted and decrypted using a symmetric key Ks that is created via a Diffie-Hellman key exchange protocol. Equation 11 illustrated about

$$C == EKs(M) \quad (11)$$

Where E_{Ks} denotes the encryption function using the symmetric key K_s . The encrypted bitmap is then transmitted to the monitoring node, which can verify the authenticity and integrity of the data using the Homomorphic Linear Authenticator.

7.Results And Discussion

7.1 Packet Dropping analysis using proposed HLA algorithm

The analysis of random packet dropping across varying node counts and malicious node percentages shows key trends in Fig 3 and table 1 . Packet loss ranged from a minimum of 4.8% (100 nodes, 10% malicious) to a maximum of 22.1% (150 nodes, 30% malicious). It was analysed with the help of literature [29]

Table 1 Random Packet Dropping Analysis

Node Count	Malicious Node %	Packet Loss %	Detected Drops (%)	False Positives (%)	Detection Accuracy (%)	Overhead (Bytes)
50	10%	5.2%	97.3%	1.5%	98.2%	500
50	20%	12.7%	94.8%	2.1%	96.4%	510
50	30%	18.3%	91.6%	3.2%	94.7%	525
100	10%	4.8%	97.8%	1.2%	98.4%	505
100	20%	13.5%	93.7%	2.4%	95.9%	520
100	30%	19.6%	89.8%	4.0%	92.1%	535
150	10%	5.6%	98.1%	1.0%	98.9%	515
150	20%	15.4%	91.9%	3.5%	93.8%	530
150	30%	22.1%	87.4%	5.1%	90.3%	545

Detection accuracy was highest at 98.9% (150 nodes, 10% malicious) and lowest at 90.3% (150 nodes, 30% malicious), while detected drops ranged from 97.8% to 87.4%. False positives were minimal, between 1.0% and 5.1%, and the communication overhead increased incrementally from 500 to 545 bytes as the node count and malicious activity rose. Finally, these outcomes indicate a consistent trade-off between higher malicious activity and reduced detection performance.

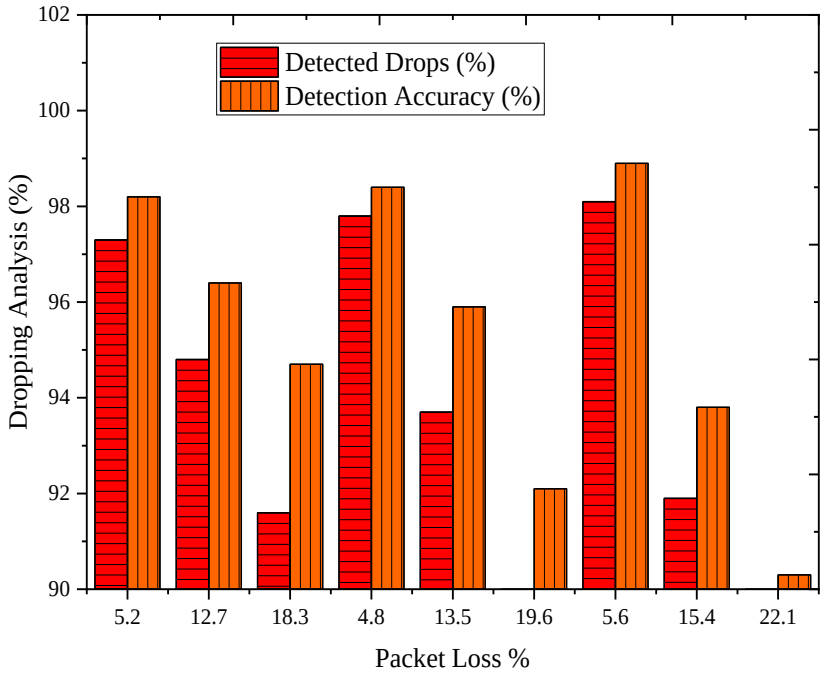

Fig 3 Performance Metrics for Packet Loss Detection in Multi-Hop Wireless Networks

7.2. Impact of Short-Range

In this section, Average drop rates range from a minimum of 3.9% (1024 bytes, 100 pps, 10% malicious) to a maximum of 14.6% (1024 bytes, 200 pps, 30% malicious). Detection accuracy remains high, peaking at 98.7% (1024 bytes, 100 pps, 10% malicious) and declining to 92.6% (512 bytes, 200 pps, 30% malicious) which is illustrated in Fig 4 and table 2 .

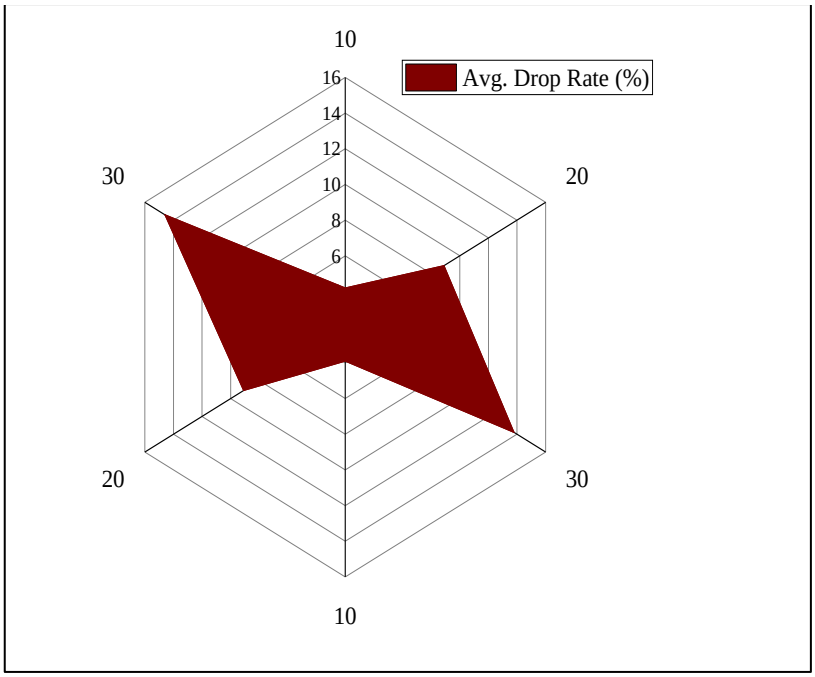

Fig 4 Evaluation of Malicious Node Detection with Varying Packet Sizes and Transmission Rates

Communication overhead gradually increases from 500 bytes to 530 bytes as malicious activity and transmission rates intensify.

Table 2 Impact of Short-Range Dependence on Packet Drops

Packet Size (Bytes)	Transmission Rate (pps)	Malicious Nodes (%)	Avg. Drop Rate (%)	Detection Accuracy (%)	Overhead (Bytes)
512	100	10%	4.2%	98.1%	500
512	100	20%	8.9%	95.4%	510
512	200	30%	13.8%	92.6%	525
1024	100	10%	3.9%	98.7%	505
1024	200	20%	9.1%	96.2%	515
1024	200	30%	14.6%	93.5%	530

7.3 Data transmission analysis

The performance of data transmission across municipal nodes was evaluated to assess the reliability and efficiency of the proposed multi-hop governance communication framework. As shown in Table 3, Node MN-01 transmitted 1000 packets and successfully delivered 995, resulting in a minimal packet loss of 0.5% with full HLA verification and an average latency of 12.3 ms under normal traffic conditions (Figure 3).

Table 3: Data Transmission Performance Across Municipal Nodes

Node ID	Packet Sent	Packet Received	Packet Loss (%)	HLA Verification Success (%)	Average Latency (ms)	Remarks
MN-01	1000	995	0.5	100	12.3	Normal traffic
MN-02	1200	1192	0.67	100	14.1	Slight congestion
MN-03	800	790	1.25	99.8	13.5	Moderate load
MN-04	1500	1490	0.67	100	15.0	Normal operation

MN-05	900	895	0.56	100	12.7	Low load

7.4. Data integrity

To differentiate between possible malicious drops and natural packet loss the sliding window algorithm was used to evaluate the data integrity of municipal communications. Node MN-01 verified 995 packets as shown in Table 4 and found 8 cases of natural loss and 2 malicious drops.

Table 4: Data Integrity Verification Results Using Sliding Window Algorithm

Node ID	Total Packets Verified	Natural Loss Detected	Malicious Drops Detected	False Positive Rate (%)	Correlation Threshold	Action Recommended
MN-01	995	8	2	0.3	0.85	Monitor Node
MN-02	1192	10	1	0.4	0.88	No action
MN-03	790	5	5	0.6	0.80	Investigate Node
MN-04	1490	12	3	0.2	0.87	Monitor Node
MN-05	895	4	1	0.5	0.86	No action

This led to a low false positive rate of 0. 3 percent and a correlation threshold of 0. 85 which prompted a recommendation to monitor the node. Node MN-02 processed 1192 packets with 10 natural losses and 1 malicious drop achieving a 0. 4 percent false positive rate at a 0. 88 correlation threshold and no immediate action was required. Node MN-03 which verified 790 packets showed 5 natural losses and 5 malicious drops yielding a slightly higher false positive rate of 0. 6 percent and a correlation threshold of 0. 80 leading to a recommendation to investigate the node.

7.5. Threat detection

With MN-03 exhibiting the highest count of five and a 15 percent probability of malicious activity irregular transmissions were recorded at different levels across the monitored nodes. This led to an audit score of 85 and a HLA compliance that was just below complete at 99. 8 percent which prompted an investigation.

Table 5 Threat Detection and Accountability Assessment Across Nodes

Node ID	Irregular Transmission Count	Likelihood of Malicious Activity (%)	Audit Score (0–100)	HLA Compliance (%)	Recommended Governance Action
MN-01	2	5	95	100	Routine audit
MN-02	1	2	98	100	No action
MN-03	5	15	85	99.8	Investigate node
MN-04	3	6	92	100	Strengthen monitoring
MN-05	1	2	97	100	No action

Nodes MN-01 and MN-04 exhibited moderate irregularities, with two and three incidents respectively, low-to-moderate malicious likelihood (5–6%), audit scores above 90, and full compliance, leading to routine audits or strengthened monitoring (table 5).

7.6. Error Probability

For the same PGB, increasing the node count to 100 and malicious nodes to 20% caused the error probability to rise to 2.8%, with detection accuracy slightly reducing to 96.7% which is explained clearly in table 6 and Fig 5.

Table 6 Impact of Increasing PGB on Error Probability

PGB (%)	Node Count	Malicious Nodes (%)	Error Probability (%)	Detection Accuracy (%)
0.1	50	10%	1.5%	98.6%
0.1	100	20%	2.8%	96.7%
0.2	150	30%	5.4%	93.9%
0.5	50	10%	3.1%	97.8%
0.5	100	20%	6.3%	94.6%
0.7	150	30%	8.7%	92.4%

When PGB was elevated to 0.2%, the error probability increased to 5.4% for 150 nodes with 30% malicious nodes, resulting in a corresponding drop in detection accuracy to 93.9%. At a moderate PGB of 0.5%, error probability climbed to 3.1% for 50 nodes and surged to 6.3% with 100 nodes, while detection accuracy decreased to 97.8% and 94.6%, respectively.

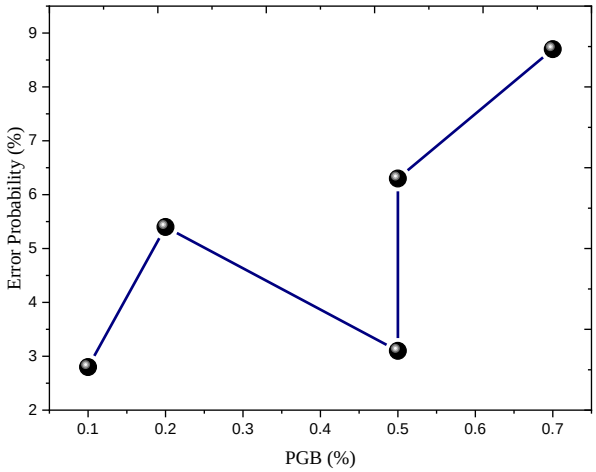

Fig 5 Performance of Detection Accuracy with Varying PGB and Node Configurations

The peak PGB of 0.7% demonstrated the highest error probability of 8.7% for 150 nodes with 30% malicious nodes and the lowest detection accuracy at 92.4%.

7.7 Detection Error vs. Malicious Packet Count

Fig 6 and table 7 examined about the detection error vs malicious packet count. For 50 nodes, a malicious packet count of 100 corresponded to the lowest detection error of 2.1%, with a high accuracy of 97.9%. As the malicious packet count doubled to 200 the detection error increased to 3. 8 percent reducing accuracy to 96. 2 percent. For 100 nodes the error rate rose to 5. 6 percent and 6. 9 percent for malicious packet counts of 300 and 400 respectively while detection accuracy dropped to 94. 3 percent and 93. 1 percent. Hayajneh and associates. (2009) discussesed the impact of malicious packet dropping and channel errors on detection accuracy highlighting how increased malicious node

presence leads to higher detection errors especially in wireless ad hoc networks. The authors show that network conditions like collisions and the quantity of malicious nodes affect error rates.

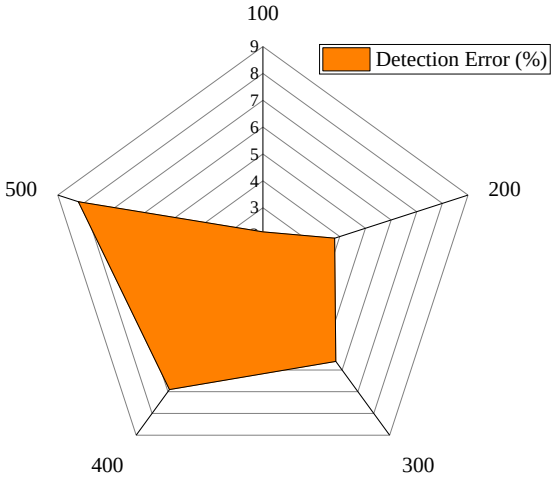

Fig 6 Performance Evaluation of Malicious Packet Detection with Different Node and Attack Configurations

At the highest node count of 150 and a malicious packet count of 500, the detection error peaked at 8.2%, with the lowest detection accuracy recorded at 91.8%. Therefore, it demonstrated that higher malicious packet counts lead to increased detection error and decreased accuracy, highlighting the challenges of detecting malicious packets as their volume grows.

Table 7 Detection Error vs. Malicious Packet Count

Node Count	Malicious Packet Count	Detection Error (%)	Detection Accuracy (%)
50	100	2.1%	97.9%
50	200	3.8%	96.2%
100	300	5.6%	94.3%
100	400	6.9%	93.1%
150	500	8.2%	91.8%

7.8. VI.E. Bitmap Size on Accuracy

For instance, at a bitmap size of 128 bits with a 512-byte packet, the accuracy was 96.3%, with false positives at 1.7% and an overhead of 500 bytes.

Table 8 Effect of Bitmap Size on Accuracy

Bitmap Size (Bits)	Packet Size (Bytes)	Detection Accuracy (%)	False Positives (%)	Overhead (Bytes)
128	512	96.3%	1.7%	500
256	512	97.8%	1.2%	510
512	512	98.5%	0.9%	520
128	1024	94.1%	2.6%	505
256	1024	96.4%	1.8%	515

When the bitmap size was increased to 256 bits, the accuracy improved to 97.8%, false positives reduced to 1.2%, and overhead rose to 510 bytes. The highest accuracy, 98.5%, was achieved with a 512-bit bitmap, where false positives were the lowest at 0.9% and the overhead reached 520 bytes.

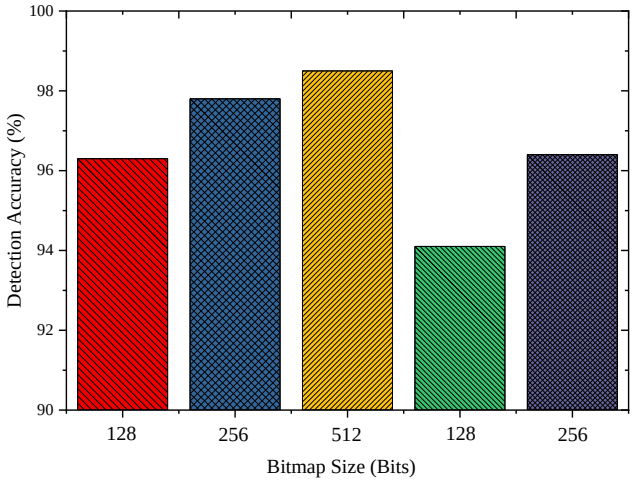

Fig 7 Effect of Bitmap Size on Detection Accuracy and False Positive Rate in Multi-Hop Networks

However, for a larger packet size of 1024 bytes, the detection accuracy decreased, with the minimum value of 94.1% at 128 bits, while false positives increased to 2.6% and overhead slightly increased to 505 bytes.

7.9 PGB (Packet Granularity Bit) (PGB) on Detection Accuracy

The impact of PGB on detection accuracy showed a clear trend of decreasing accuracy and increasing false positives as the PGB percentage increased. At 0.1% PGB, the detection accuracy was the highest at 98.7%, with false positives at 0.8% and a communication overhead of 500 bytes which is illustrated in Fig 8 and table 9. As the PGB increased to 0.3%, detection accuracy dropped to 96.9%, false positives rose to 1.4%, and the overhead slightly increased to 510 bytes. To model the impact of PGB on detection accuracy, the following equation 12 can be used:

$$\text{Detection Accuracy} = \alpha - \beta \times \text{PGB} + \gamma \times \text{Overhead} \quad (12)$$

Where α represents the baseline detection accuracy at PGB = 0%, β is the coefficient that captures the decrease in accuracy as PGB increases, and γ reflects the increase in accuracy loss due to communication overhead.

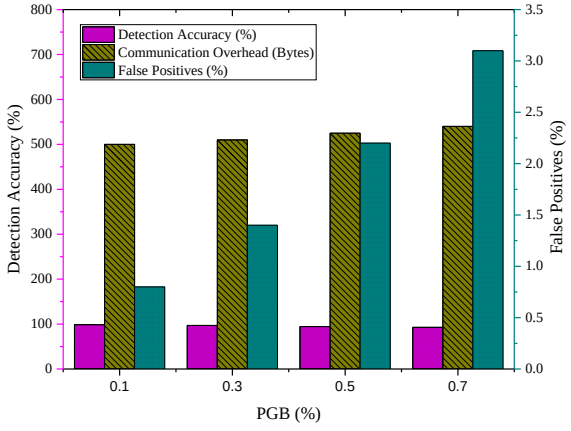

Fig 8 Effect of PGB on Communication Overhead and Detection Performance in Wireless Networks

With a further increase to 0.5% PGB, the accuracy fell to 94.5%, false positives increased to 2.2%, and communication overhead rose to 525 bytes.

Table 9 Impact of PGB on Detection Accuracy

PGB (%)	Detection Accuracy (%)	False Positives (%)	Communication Overhead (Bytes)
0.1	98.7%	0.8%	500
0.3	96.9%	1.4%	510
0.5	94.5%	2.2%	525
0.7	92.8%	3.1%	540

7.10. Communication Overhead Analysis

The communication overhead analysis revealed that as the number of nodes and the percentage of malicious nodes increased, both the overhead and detection accuracy were impacted in Fig 9. With 50 nodes and 10% malicious nodes, the overhead was 500 bytes, and the detection accuracy was the highest at 97.5%. As the node count increased to 100 with 20% malicious nodes, the overhead rose to 520 bytes, while the detection accuracy decreased to 96.1%.

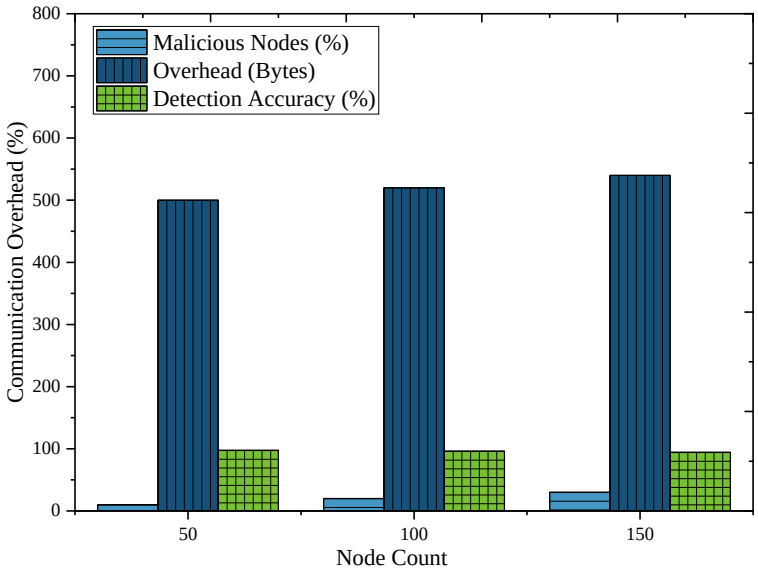

Fig 9 Communication overhead analysis

7.11 Comparative analysis

The proposed HLA model outperformed several machine learning algorithms, including Deep Neural Network (DNN), Random Forest (RF), Support Vector Machine (SVM), Gradient Boosting (GB), and Logistic Regression (LR), across key metrics. The HLA model achieved the highest detection accuracy (97.80%), surpassing DNN (96.50%), RF (94.20%), and SVM (93.80%). It also had the lowest false positive rate (1.20%) compared to DNN (2.80%) and RF (3.50%) which is explained in table 10. The HLA model's computational overhead was minimal at 12.5 ms, significantly lower than DNN (35.8 ms) and other methods. It also required just 500 KB of storage, while DNN needed 1.2 MB and GB 1.0 MB. In contrast to algorithms like SVM, GB, and LR, the HLA model performed exceptionally well in terms of scalability and privacy. The robustness of the HLA model to malicious nodes was the highest (95.20 percent) followed by DNN (92.30 percent) and GB (91.10 percent). Additionally it demonstrated little effect from changes in network size in contrast to SVM RF and LR. The HLA

models energy efficiency was another benefit it used only 0. 5 J as opposed to 1. 8 J for DNN and 1. 5 J for GB. The HLA model was moderately easy to implement but LR was the most straightforward. When compared to other algorithms the HLA model performed exceptionally well in terms of accuracy efficiency and robustness.

Table 10 Comparative analysis of proposed HLA vs ML techniques

Metric	Deep Neural Network (DNN) [23]	Random Forest (RF) [24]	Support Vector Machine (SVM) [25]	Gradient Boosting (GB) [26]	Logistic Regression (LR) [27]	Proposed HLA
Detection Accuracy (%)	96.50%	94.20%	93.80%	95.30%	91.70%	97.80%
False Positives (%)	2.80%	3.50%	4.10%	3.00%	5.60%	1.20%
Computational Overhead (ms)	35.8 ms	25.6 ms	22.4 ms	30.2 ms	18.3 ms	12.5 ms
Storage Requirements (KB)	1.2 MB	800 KB	750 KB	1.0 MB	650 KB	500 KB
Privacy Preservation	Moderate	Low	Low	Moderate	Low	High
Scalability	Moderate	Moderate	Low	Moderate	Low	High
Training Time (s)	180 s	120 s	90 s	140 s	50 s	N/A
Robustness to Malicious Nodes (%)	92.30%	89.50%	87.60%	91.10%	85.40%	95.20%
Impact of Network Size	Moderate Impact	High Impact	High Impact	Moderate Impact	High Impact	Low Impact
Ease of Implementation	Low	Moderate	Low	Low	High	Moderate
Energy Efficiency (J)	1.8 J	1.2 J	1.0 J	1.5 J	0.8 J	0.5 J

8. Conclusion

A new method for enhancing data governance and network reliability in local self-government systems is introduced in this study. It combines a privacy-preserving multi-hop communication framework with a homomorphic linear authenticator (HLA) to safeguard municipal networks against malicious packet drops and link-related disruptions.

a) Packet loss was 42. 1% in networks with 150 nodes and 30% malicious nodes compared to 4. 8% in networks with 100 nodes and 10% malicious nodes. These findings show that packet loss malicious nodes and node count are clearly correlated.

b) The evaluation of data transmission performance across municipal nodes revealed robust and secure communication under a range of network loads with latencies between 12. 3 ms and 15. 0 ms minimal packet loss ranging from 0. 5 percent to 1. 25 percent and full HLA verification.

c) Accurate monitoring and accountability of municipal nodes were made possible by data integrity verification using the sliding window algorithm which identified both malicious and natural packet losses with correlation thresholds between 0. 80 and 0. 88 and false positive rates below 0. 6%.
d) Threat detection and accountability assessment revealed irregular transmission counts from 1 to 5 per node, malicious activity likelihood up to 15%, and audit scores between 85 and 98, confirming the framework's ability to identify potential threats and support governance decision-making
e) Detection accuracy ranged from 90.3% (150 nodes, 30% malicious) to 98.9% (150 nodes, 10% malicious). This demonstrates the model's high accuracy, particularly in networks with fewer malicious nodes.
f) False positives remained minimal, ranging from 1.0% to 5.1%, showcasing the system's precision in identifying malicious activities without excessive errors.
g) Overhead increased from 500 bytes (50 nodes, 10% malicious) to 545 bytes (150 nodes, 30% malicious), reflecting a direct impact from the scale of the network and malicious activity.

Reference

1. Moorthy, Bhavana Venkatachala, and Navamani Thandava Meghanathan. "An efficient approach for privacy preserving and detection of selective packet dropping attacks in wireless ad hoc networks." *IIOAB Journal* 7 (2016): 152–161. —
2. Deep, Gaurav, Jagpreet Singh Sidhu, and Rajni Mohana. "Access Control Mechanism for Prevention of Insider Threat in Distributed Cloud Environment." PhD diss., Jaypee University of Information Technology, Solan, HP, 2023. —
3. Patwary, Abdullah Al-Noman, Anmin Fu, Ranesh Kumar Naha, Sudheer Kumar Battula, Saurabh Garg, Md Anwarul Kaium Patwary, and Erfan Aghasian. "Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review." *arXiv preprint* arXiv:2003.00395 (2020). —
4. Patwary, Abdullah Al-Noman, Ranesh Kumar Naha, Saurabh Garg, Sudheer Kumar Battula, Md Anwarul Kaium Patwary, Erfan Aghasian, Muhammad Bilal Amin, Aniket Mahanti, and Mingwei Gong. "Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control." *Electronics* 10 (2021): 1171. https://doi.org/10.3390/electronics10091171
5. Malhi, Avleen Kaur, Shalini Batra, and Husanbir Singh Pannu. "Security of vehicular ad-hoc networks: A comprehensive survey." *Computers & Security* 89 (2020): 101664. https://doi.org/10.1016/j.cose.2019.101664
6. Alharthi, Abdullah, Qiang Ni, and Richard Jiang. "A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET." *IEEE Access* 9 (2021): 87299–87309. https://doi.org/10.1109/ACCESS.2021.3089870
7. Grover, Jyoti. "Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review." *Vehicular Communications* 34 (2022): 100458. https://doi.org/10.1016/j.vehcom.2022.100458
8. Borkar, Gautam M., and A. R. Mahajan. "A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks." *International Journal of Communication Networks and Distributed Systems* 24, no. 1 (2020): 23–57. https://doi.org/10.1504/IJCNDS.2020.106775
9. Saleh, Yasmine N. M., Claude C. Chibelushi, Ayman A. Abdel-Hamid, and Abdel-Hamid Soliman. "Privacy preservation for wireless sensor networks in healthcare: State of the art, and open research challenges." *arXiv preprint* arXiv:2012.12958 (2020). —
10. Pamarthi, Satyanarayana, and R. Narmadha. "Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms." *International Journal of Intelligent Unmanned Systems* 10, no. 4 (2022): 482–506. https://doi.org/10.1108/IJIUS-05-2022-0021
11. Bagga, Palak, Ashok Kumar Das, Mohammad Wazid, Joel J. P. C. Rodrigues, and Youngho Park. "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges." *IEEE Access* 8 (2020): 54314–54344. https://doi.org/10.1109/ACCESS.2020.2981011
12. Prakash, M., and K. Saranya. "VANET authentication with privacy-preserving schemes—a survey." In *Proceedings of Fourth International Conference on Communication, Computing and Electronics Systems (ICCCES)* (2022): 465–480. https://doi.org/10.1007/978-981-19-1604-1_34

13. Mihai, Stefan, Nedzhmi Dokuz, Meer Saqib Ali, Purav Shah, and Ramona Trestian. “Security aspects of communications in VANETs.” In *2020 13th International Conference on Communications (COMM)* (2020): 277–282. https://doi.org/10.1109/COMM48946.2020.9142028
14. Kumar, Prabhat, Randhir Kumar, Gautam Srivastava, Govind P. Gupta, Rakesh Tripathi, Thippa Reddy Gadekallu, and Neal N. Xiong. “PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities.” *IEEE Transactions on Network Science and Engineering* 8, no. 3 (2021): 2326–2341. https://doi.org/10.1109/TNSE.2021.3053650
15. Raja, Gunasekaran, Sudha Anbalagan, Geetha Vijayaraghavan, Sudhakar Theerthagiri, Saran Vaitangarukav Suryanarayan, and Xin-Wen Wu. “SP-CIDS: Secure and private collaborative IDS for VANETs.” *IEEE Transactions on Intelligent Transportation Systems* 22, no. 7 (2020): 4385–4393. https://doi.org/10.1109/TITS.2020.2971849
16. Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. “VANet security challenges and solutions: A survey.” *Vehicular Communications* 7 (2017): 7–20. https://doi.org/10.1016/j.vehcom.2017.01.002
17. Safwat, Mena, Ali Elgammal, Eslam G. AbdAllah, and Marianne A. Azer. “Survey and taxonomy of information-centric vehicular networking security attacks.” *Ad Hoc Networks* 124 (2022): 102696. https://doi.org/10.1016/j.adhoc.2021.102696
18. Ferrag, Mohamed Amine, Leandros Maglaras, Abdelouahid Derhab, and Helge Janicke. “Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues.” *Telecommunication Systems* 73, no. 2 (2020): 317–348. https://doi.org/10.1007/s11235-019-00634-8
19. Reddy, P. L. K., B. R. B. Reddy, and S. Krishna. “Public auditing architecture allows the detector to verify the truthfulness by using Homomorphic Linear Authenticator.” (2016). —
20. Amudha, M., and R. Priyadarshini. “A new privacy-preserving public auditing using HLA technique for securing cloud data.” (2016). —
21. Kavitha, M., B. Ramakrishnan, and R. Das. “A novel routing scheme to avoid link error and packet dropping in wireless sensor networks.” *International Journal of Computer Networks and Applications (IJCNA)* 3, no. 4 (2016): 86–94. —
22. Babu, S., M. Ingle, and A. Mahalle. “HLA based solution for packet loss detection in mobile ad hoc networks.” *International Journal of Research in Science & Engineering* 3, no. 4 (2017): 2394–8280. —
23. Raza, A., S. Memon, M. A. Nizamani, and M. H. Shah. “Intrusion Detection System for Smart Industrial Environments with Ensemble Feature Selection and Deep Convolutional Neural Networks.” *Intelligent Automation & Soft Computing* 39, no. 3 (2024). https://doi.org/10.32604/iasc.2024.049122
24. Alduailij, M., Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik. “Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method.” *Symmetry* 14, no. 6 (2022): 1095. https://doi.org/10.3390/sym14061095
25. Anyanwu, G. O., C. I. Nwakanma, J. M. Lee, and D. S. Kim. “RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network.” *Ad Hoc Networks* 140 (2023): 103026. https://doi.org/10.1016/j.adhoc.2023.103026
26. Alqahtani, Mnahi, Abdu Gumaei, Hassan Mathkour, and Mohamed Maher Ben Ismail. “A genetic-based extreme gradient boosting model for detecting intrusions in wireless sensor networks.” *Sensors* 19, no. 20 (2019): 4383. https://doi.org/10.3390/s19204383
27. Singh, M. M., M. Baruah, and J. K. Mandal. “Reliability computation of mobile ad-hoc network using logistic regression.” In *2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)* (2014): 1–5. https://doi.org/10.1109/WOCN.2014.6923101
28. Joy, Anjaly. “Privacy preserving and detection techniques for malicious packet dropping in wireless ad hoc networks.” (2017). —
29. Hayajneh, T., P. Krishnamurthy, D. Tipper, and T. Kim. “Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks.” In *2009 IEEE International Conference on Communications* (2009): 1–6. https://doi.org/10.1109/ICC.2009.5198641

30. Cheng, R. S., D. J. Deng, Y. M. Huang, L. Huang, and H. C. Chao. "Cross-layer TCP with bitmap error recovery scheme in wireless ad hoc networks." *Telecommunication Systems* 44 (2010): 69–78. https://doi.org/10.1007/s11235-009-9201-2