International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Irregularity Behaviour Detection - Ad-hoc On-Demand Distance Vector Routing Protocol (IBD - AODV): A Novel Method for Determining Unusual Behaviour in Mobile Ad-hoc Networks (MANET)

N. Kanimozhi[1], Dr. S. Hari Ganesh[2], Dr. B. Karthikeyan[3]
[1]Research Scholar,
Department of Computer Science,
H.H The Rajah's College (Affiliated to Bharathidasan University, Tiruchirappalli),
Pudukkotai – 622 001.
nkanimozhimphil@gmail.com
[2]Assistant Professor,
Department of Computer Science,
H.H The Rajah's College (Affiliated to Bharathidasan University, Tiruchirappalli),
Pudukkotai – 622 001.
hariganesh17@gmail.com
[3]Associate Professor,
Department of Computer Science,
Bishop Heber College (Affiliated to Bharathidasan University, Tiruchirappalli),
Trichy – 620 017.
bkarthikeyanphd@gmail.com

Abstract*:* All the communication in the mobile ad-hoc network (MANET) will depend on the intermediate neighbour nodes or router nodes. Routing protocol is very important in MANET, because all the communication will be done in the MANET depending on the neighbour or intermediate node. If the intermediate node is a malicious node, all the data will be lost or changed by the intermediate or malicious node. Ad-hoc On-demand Distance Vector routing protocol is one of the moderate routing protocol in MANET. The Ad-hoc On-demand Distance Vector Routing protocol does not have any security mechanism. This work is going to find the Irregularity Behaviour Detection (IBD) over the Ad-hoc On-Demand Distance Vector Routing (AODV) protocol. IBD is finding a trusted node by using the trust value (TV) of the node. This TV includes network performance, node energy level, and node position value. IBD-AODV is implemented and tested in the OmNetpp 6.0 simulator.

Keywords: MANET, Intermediate node, Routing, Trust Value, Network Performance, AODV, IBD-AODV, Network performance, Node energy level, OmNetpp.

1. Introduction

Mobile devices can connect with one another in a mobile ad hoc network (MANET) without the aid of any pre-existing infrastructure, such as base stations or centralised access points. Because nodes can join or leave a MANET at any time, the topology of the network can vary quickly. This characteristic of MANETs is known as its dynamic nature.

Each component of a MANET, known as a node, serves as a router and is in charge of sending data packets to other nodes. In order to reach farther-off destinations, nodes in the network can either create direct communication links or use intermediary nodes as relays. The ability for nodes to relay data through multiple hops allows the MANET to extend its coverage over a broader geographic area and enables communication among devices that are located beyond their direct wireless reach.

MANETs are utilized in scenarios where establishing a fixed infrastructure is challenging or impractical, such as disaster-stricken areas, military operations, or collaborative environments that are formed spontaneously. They provide flexible and resilient communication capabilities, allowing devices to establish connections while on the move and adapt to changing network conditions.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

The routing protocols implemented in MANETs are specifically designed to tackle the distinct challenges posed by the dynamic nature of the network. These protocols play a crucial role in route discovery, maintaining network connectivity, and efficiently adapting to topology changes. Additionally, they strive to minimize overhead and conserve network resources.

Some well-known MANET routing protocols are as follows:

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol characterized as reactive, as it establishes routes between nodes as and when required. It initiates route discovery solely when there is a demand and maintains these routes as long as they remain in use.

AODV, a reactive protocol, utilizes the hop-to-hop routing approach. When a node wants to find a route to a specific destination, it sends route requests (RREQs) in AODV. As these RREQs are forwarded by intermediary nodes, the target node also receives a reverse route. To provide the complete route to the destination, the target node generates a route reply (RREP) upon receiving the route request, including all the necessary hops. By employing on-demand routing, AODV reduces the delay in establishing connections. Sequence numbers are used to determine the most recent routes. However, AODV may generate multiple route reply packets in response to a single route request packet, resulting in significant control overhead.

Dynamic Source Routing (DSR) is a reactive protocol that operates based on source routing. It enables each data packet to contain all the necessary route information to reach its destination, eliminating the requirement for the network to maintain routing tables.

Optimized Link State Routing (OLSR) is a proactive routing protocol that keeps pre-computed routes to all nodes within the network. It achieves this by periodically exchanging topology information, which helps update and optimize the routes.

Destination-Sequenced Distance Vector (DSDV) is a proactive protocol that utilizes the traditional distance vector algorithm. It manages a routing table containing sequence numbers to guarantee loop-free and current routing information.

A mobile ad-hoc network (MANET) is a wireless network without any fixed infrastructure, allowing communication between mobile devices anywhere and anytime. When a source node needs to communicate with a destination, a MANET forms by a group of mobile devices. In this network, each node acts as a source, destination, and router, making routing between source and destination challenging in mobile node networks.

MANET utilizes three different routing protocols: reactive, proactive, and hybrid. Based on previous research, Proactive AODV is considered a moderate protocol for MANET. Although AODV lacks prevention techniques, it demonstrates moderate performance in terms of packet delivery ratio (PDR) and end-to-end time delay (EETD). This work combines the IBD algorithm with AODV to establish a trust value-based trusted node group.

Finding anomalous activity or events within the network is the first step in anomaly detection in Mobile Ad-Hoc Networks (MANETs). Anomaly detection is difficult with MANETs due to their dynamic topology, constrained resources, and lack of a centralised infrastructure.

Finding anomalies from expected node behaviour, routing protocols, or network traffic patterns is the aim of anomaly detection algorithms in MANETs. MANET anomalies can be caused by nefarious assaults, node failures, routing issues, or odd network behaviour.

Anomaly detection in MANETs use a variety of techniques, including:

Statistically based approaches: These strategies use statistical tools like mean, standard deviation, or outlier identification algorithms to analyse network metrics, traffic patterns, or node behaviour to find anomalies.

Machine learning-based strategies: To learn the typical network behaviour and spot anomalies, machine learning algorithms can be trained on labelled data. To find deviations from typical patterns, methods like clustering, classification, or anomaly scoring algorithms are used.

Trust-based strategies: These techniques create bonds of trust between network nodes. Anomalies are discovered by locating departures from predicted trust levels. Nodes share trust information based on their observations and behaviour.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Rule-based strategies: To find abnormalities, rule-based systems use established rules or heuristics. These guidelines are predicated on particular network restrictions, protocol requirements, or recognised attack patterns.

Due to the dynamic nature of the network and the limited amount of resources available, detecting abnormalities in MANETs is a challenging operation. To efficiently identify abnormalities and mitigate potential risks or disruptions, network parameters, traffic patterns, and the particular qualities of MANET settings must be carefully taken into account.

2. Literature Review

In MANETs, outsider may be introduced by a number of factors, including hardware/software , the environment , a deviation from a standard system configuration for security , or data uncertainty [4,5]. These anomalies can be categorised as statistics or knowledge-driven [6], built using Markov or hidden-Markov models [7, 8], connected to density [9, 10], affected by distance [12, 13], or defined as global, semiglobal, or distributed anomalies [14, 15]. These outsiders can emerge at various levels within the MANET, including individual nodes, data elements, or the overall network itself.

The most common method for dealing with statistical/knowledge-based outliers is based on building probabilistic data models utilising applied statistics and probability concept mathematical approaches. Utilising measuring techniques, the statistically based stranger detection system analyses user behaviours. According to the definition of a Markov chain, which is a random method of discrete state space, the following state depends only on the present state and is unrelated to how the system arrived at the present state. The Markov chain is typically used to build a normal profile that represents the temporal relationship among network activity [8].

The density-based strategy, first put forth by Breunig et al. [9], entails evaluating the input key density distributions and locating outliers in low-density areas [10]. This approach also looks at various data points in designated locations that can be identified for distance-based outlier detection in congested areas [11]. For these distance-based detections, geometric distances that can be translated into terms of objects are estimated. A function F that may be expressed by the formula F: x R is given for each outlier factor, where an item x from a collection of objects can be recognised as an outlier in R. [12–14] provides an overview of several definitions frequently used in relation to distance-based outlier detection.

In their work, Venkana et al. [23] focused on the isolation of malicious nodes by employing the trust-and-energy-based ad hoc on-demand distance vector (AODV) technique. This approach dynamically calculates the trust and energy values of nodes within the network topology, aiming to improve the packet delivery rate and reduce the typical end-to-end delay associated with the routing performance of the AODV algorithm. Through their proposed method, Shan et al. [24] successfully detected selfish nodes and conducted a quantitative analysis of the impact of node selfishness, resulting from energy depletion, on packet loss rate, throughput, and round-trip time within MANETs.

Mean clustering techniques were used by Gopal Krishnan et al. [25] to create a power-saving management system for MANETs. Compared to other approaches, such transmission and direct communication protocols, their strategy reduced power and energy loss. The effectiveness of their suggested solution in lowering energy dissipation within MANETs was shown by experimental data. Abdulmunem et al.'s discussion of resource limitations in MANETs emphasised the difficulties brought on by these networks' low energy and short system lifetimes. They investigated protocols like the lowest identifier clustering algorithm (LIDCA) and the greatest degree Throughput, Network Lifetime, and Packet Delivery Ratio of the clustering method (HDCA). Their simulation results showed that their innovative clustering algorithm enabled efficient energy distribution and surpassed HDCA and LIDCA in terms of network longevity. Red Deer Algorithm (RDA)-based Energy-Efficient QoS Routing for MANETs (RDA-EQRP) was proposed by Arivarasan et al. Apart from providing support for dependability, bandwidth, static resource capacity, quality, and delay, RDA (Reliability and Delay Aware) routing algorithm aims to find the shortest path between a source and destination while also considering energy preservation. Through simulations, it has been observed that the proposed RDA-EQRP (Energy and Quality of Routing Protocol) consumes less energy in MANET routing.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

3. Proposed Work : Irregularity Behaviour Detection (IBD)

A method of discovering anomalies in a system or network based on trust relationships among its constituents is known as "trust-based anomaly detection." By observing and assessing the behaviours, relationships, and reputation of the entities within the system, trust is developed. By locating departures from the normal or trusted behaviour, anomalies are found.

Entities inside a system, such as nodes in a network or users in a community, build trust levels depending on a variety of parameters in trust-based anomaly detection. These elements could be past conduct, reputation, referrals from reliable sources, or explicit trust measures. Each entity develops a trust model or trust network by exchanging trust information and seeing how other entities behave.

An entity is regarded as anomalous when it significantly deviates from the expected behaviour or when its level of trust drops below a predetermined threshold. To find these discrepancies and flag them as anomalies, trust-based anomaly detection considers the connections of trust between entities.

Various sectors, including dispersed networks like Mobile Ad-Hoc Networks (MANETs), collaborative systems, and online social networks, can use trust-based anomaly detection. It has the benefit of utilising trust data to identify abnormalities, thereby improving the precision and efficiency of the detection procedure.

The formation and maintenance of trust relationships, the impact of false positives or false negatives, and the possibility for manipulation or exploitation of trust systems are some of the difficulties that trust-based anomaly detection must overcome. To provide trustworthy and accurate anomaly detection based on trust, careful design, calibration, and validation are required.In the proposed Irregularity Behaviour Detection (IBD) algorithm, each mobile device in the network will create a group (cluster) for trusted mobile devices. So initially, the proposed IBD algorithm will find whether the neighbouring device is trusted or not, and for that, IBD has to find whether the device is in the trusted group. For finding node trust, the following steps carry over from the proposed IBD:

To detect the outside in MANET, the group zones are observed. The proposed IBD proposes one session to observe the chosen area (Ac) during the period from the clock start time (CT_s) to the clock end time (CT_e).

A session (slot) may be days, months, or years. A session (Time Slot Window (TS_w)) is calculated in the following method:

$$TS_w = (CT_s, CT_e) \tag{1}$$

If the Time Slot Window (session) is days, then:

$$CT_w^{s-d} \in \{(CT_s^1, CT_e^1), (CT_s^2, CT_e^2), \dots\dots\dots, (CT_s^n, CT_e^n)\} \tag{2}$$

In a similar vein,

Month

$$CT_w^{s-m} \tag{3}$$

Year

$$CT_w^{s-y} \tag{4}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: 25 July 2023 Revised: 12 September 2023 Accepted: 30 September 2023

The suggested IBD algorithm stays away from dangerous outer values that rise as time and performance get up. Steps taken by outsiders' are as follows:

Step 1: Determine the likelihood of discovering a device in a chosen area (Ac).

The probability that node "D_m" will be found in a regular area "Ac" during the duration of:

$$CT_{Frame} \in \{CT_w^{n-d}, CT_w^{n-m}, CT_w^{s-d}\} \tag{5}$$

CT_W per CT_{Frame} in the static slot is calculated as:

$$P_{r_{St}}^{Avg} = \left(1/(CT_{Frame} - 1) \sum_{v=1, v=w}^{W} P_{r_{st}}(D_m, A_c, CT_w^v)\right) \tag{6}$$

Step 2: Determine the probability of discovering a node in an anticipated "Ac" With timestamp Ti_s, the predicted presence is calculated as follows:

$$P_{r_{St}}^{Avg} = \left(\frac{1}{CT_{Frame} - 1}\right)\left(\sum_{v=1, v=w}^{W} D_{m_{A_1}}^{((a_1^s, b_1^s)\ldots\ldots(a_1^n, b_1^n))} || D_{m_{P_1}}^{((a_1^s, b_1^s)\ldots\ldots(a_1^n, b_1^n))} . pr_{a_1 a_2} pr_{a_2 a_3} \ldots pr_{a_{n-1} a_n}, Ac, (CT_W^{T_s} \ldots\ldots CT_W^{T_s})_v\right) \tag{7}$$

In a stochastic model, which describes a series of potential events where each event's probability is solely dependent on its state,

Step 3: Find external device using Trusted Value

In a MANET, a device may be a source, intermediate device, switching device, or destination. So these devices are active ($D_{m_{A'}}$). Sometimes, due to other factors, it may be asleep or switched off; at that time, it is passive (D_{m_P}). Trust values for active and passive states are calculated as follows:

$$Trust\ Value = \left(D_{m_A}^{At} - \left(AVG_{D_{mA}+D_{mSLEEP}}^{At}\right)\right)/SD \tag{8}$$

Standard Deviation (SD) is calculated as:

$$Avg = \sum_{k=0}^{n} \frac{St.RR_k}{n} \tag{9}$$

$$Ve = \sum_{k=0}^{n} \frac{(RR_k - Avg)^2}{n} \tag{10}$$

$$SD = \sqrt{Ve} \tag{11}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

a. IBD Algorithm

i. Group Head Selection and Group Outside calculate algorithm

Select a node from MANet and calculate all the nodes energy level which is in the node's radio transmission range and assign value to D_e array.

```
Gr_Head=MAX(De)
En_T=80% of Gr_Head Energy;
Dis_T=(Gr_Head.RadioTrRange/4) *3;
Loop i=s to n
{
If ((RREP(Device(i)>En_T) && (RREP(Device(i)>Dis_T))
{
        Alert Gr_Head and avoid routing through this node
}
Else
{
        Find Current Energy;
        Find Current Position;
}
}
```

The Irregularity Behaviour Detection algorithm consists of two sub-algorithms. The first algorithm is responsible for determining the Group Head selection, while also calculating the group boundary. This algorithm identifies which devices qualify as Group Heads and calculates the boundary of the group.

The second algorithm is utilized to determine the trust value of devices within the network. By analyzing network behavior and patterns, this algorithm assigns a trust value to each device. This trust value serves as an indication of the device's reliability and integrity within the network.

Finally, based on the computed trust values, the algorithm evaluates whether a device should be categorized as within the group, outside the group, or situated on the group boundary. This decision is made by comparing the trust value of the device to predefined thresholds or criteria established by the algorithm.

ii. Trust Value is calculated by the use of following algorithm

```
Start:
        If ((D_RErr_D) > PerNegValue)
        {
                Loop(D_Err < PerNegValue)
                {
                        iv=1;
                        if (iv==0)
                        {
                                ETV=PTV;
                        }
                        Else
                        {
                                ETV=2 X ETV;
```

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

```
                        }
                }
        }
        Elseif (((PTV-ETV) < NWSD) || ((NW_Prop > PerPosValue) &&
                 (NW_Cap < PerNegValue)))
        {
                PTV=SDUT_PTV;
                ETV=PTV;
        }
        Else
        {
                No change in the Trust Value
        }
End:
```

4. Simulator Parameters

Table 1: Simulation Parameters

Parameters	Value
Numbers of Nodes	100-500
Dimension	1000mX1000m
Max Packet in queue	50
Antenna	Omni antenna
Data rates	5 packets/second
Packet size	512 bits
Mobility Model	Random waypoint mobility
Time of each slot	10 ms
Velocity(min to max)	0.3 – 5 m/s
Simulator	OmNet++ 6.0
Simulation time	600 s
Protocols	AODV, IBD AODV

The table provided enumerates approximately twelve parameters that are required by OmNetpp.

5. Methodology

a. Packet Delivery Ratio(PDR)

$$PDR = \frac{Number\ of\ Packet\ received}{Number\ of\ Packet\ Sent} \quad (12)$$

The equation 11 is used to calculate the Packet Delivery Ratio (PDR), which is determined by finding the ratio between the number of packets sent by the source and the number of packets received by the destination.

The following equation is utilized to calculate the end-to-end time delay. It measures the time difference between the packet's received time and its sent time.

b. End-to-End Time Delay (EETD)

$$EETD = Packet\ Received\ Time - Packet\ Sent\ time \quad (13)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

6. Result and Discussion

a. Packet Delivery Ratio (PDR) comparison between AODV and IBD AODV

Table 2: PDR comparison between AODV and IBD AODV

Number of Nodes	AODV	IBD-AODV
100	62	74
200	70	82
300	67	82
400	71	86
500	87	94

The proposed IBD algorithm produces a moderate packet delivery ratio (PDR). This algorithm finds Trust devices within Group Head radio transmission range. But the security of communication between source and destination is very poor. So that it gives moderate PDR.

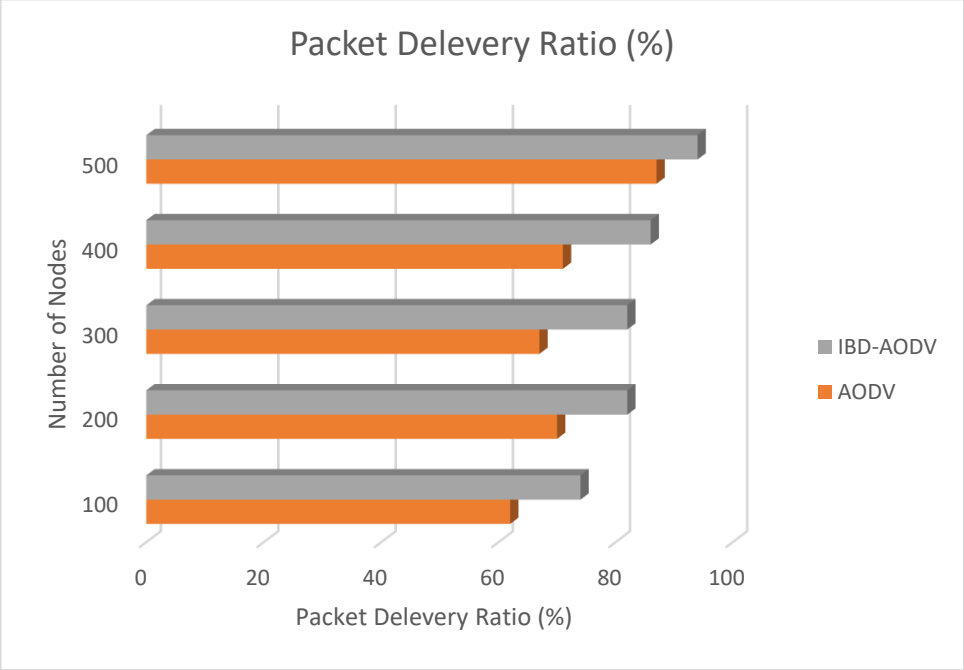

Figure 2: PDR comparison between AODV and IBD AODV

b. End-To-End Time Delay (EETD) comparison between AODV and IBD AODV

Table 3: EETD comparison between AODV and IBD AODV

Number of Nodes	AODV	IBD-AODV
100	13.822	11.518
200	15.602	13.002
300	16.262	16.426
400	26.185	21.821
500	26.46	22.05

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

The proposed IBD algorithm produces a little bit higher end-to-end time delay (EETD). This algorithm finds trust devices within Group Head radio transmission range, so it increases NRL. Due to this, it takes a little bit longer to reach the destination.

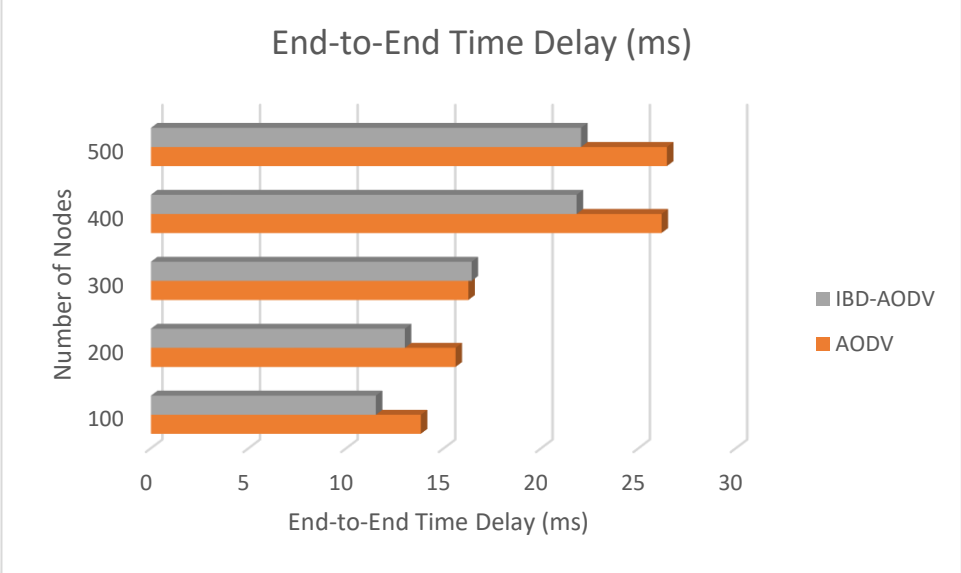

Figure 3: EETD comparison between AODV and IBD AODV

c. Comparative Analysis of Detection Ratios

i. IBDR (Irregularity Behaviour Detection Ratio)

$$IBDR = \frac{\text{Irregularity Behaviour Detected by the System}}{Number\ of\ Irregular\ Behaviour\ in\ OmNet\ Log\ file} \quad (12)$$

ii. Wrongly calculated Irregularity Behaviour Detection Ratio (W-IBDR)

$$\text{W} - \text{IBDR} = \text{Number of Device wrongly calculated as Trusted device} \quad (13)$$

The above two ratios show the real application of the IBD algorithm. Eq. 12 is used to find the irregular behaviour detection ratio in different scenarios. Here, scenario defines the number of nodes.

Eq.13 is used to find the false detection ratio of irregular behaviour detection. This factor is very important to determine how far proposed work has the wrong detection.

d. Comparative analysis of detection ratios with variations in the number of Nodes

Table 4: Comparative analysis of detection ration

No. of Nodes	**100**	**200**	**300**	**400**	**500**
IBDR	71.25	68.92	69.07	67.62	75.33
W-IBDR	7.12	8.48	10.22	12.52	14.01

The aforementioned table compares the working process of IBD with various network device counts. This finding indicates that as the number of devices rises, irregular behaviour detection operates as intended and algorithmic false detection rises correspondingly.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

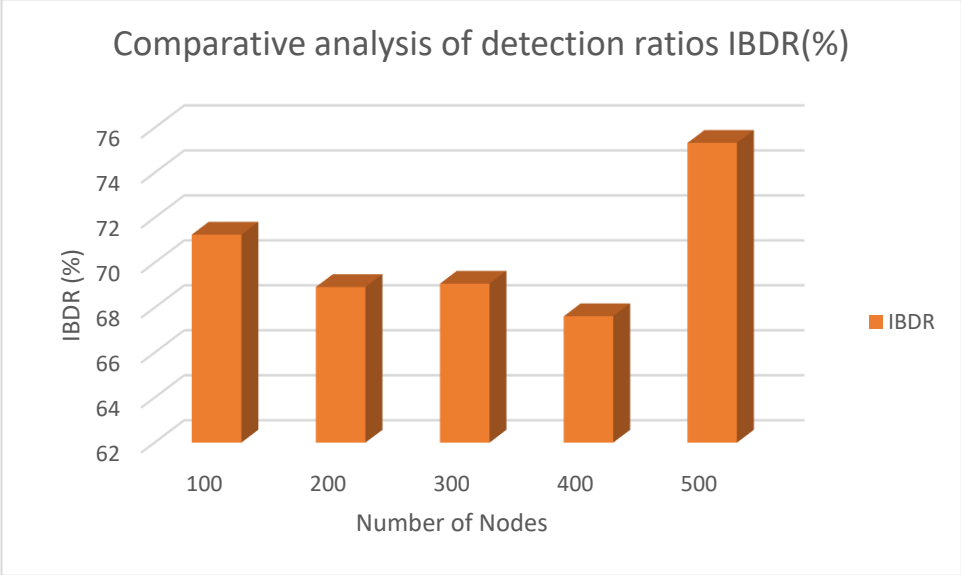

Figure 4: Comparative analysis of detection ratio

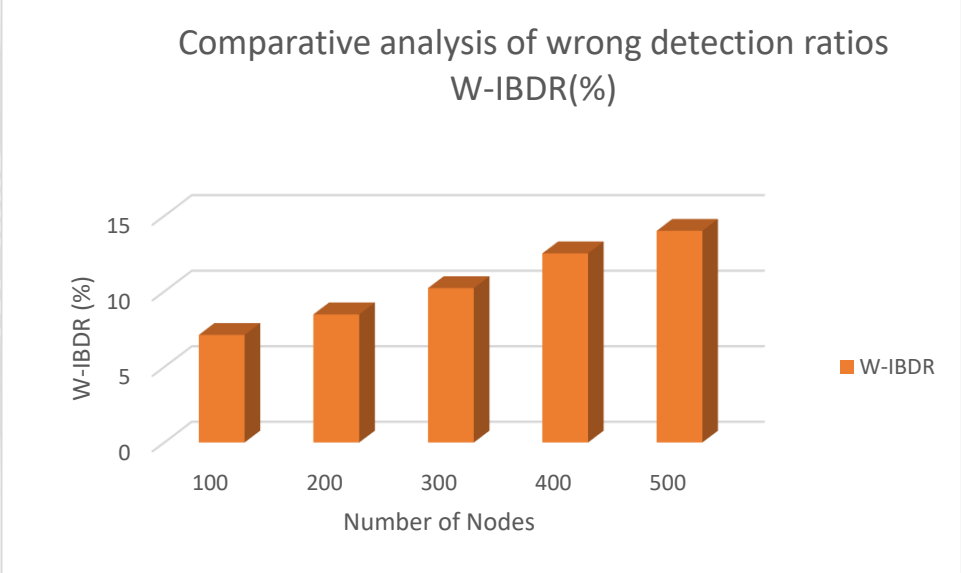

Figure 5: Comparative analysis of wrongly detection ratio

e. Comparative detection ratio analysis using different algorithm with 500 nodes.

Table 5: Comparative detection ratio analysis using different algorithms with 500 nodes

Parameter	Yang et al. [2]	Branch et al. [3]	Neeraj Chugh et al. [1]	Proposed Algorithm
IBDR	47.20%	56.60%	65.50%	75.33%
W- IBDR	8.70%	9.78%	15.15%	14.01%

This comparison contrasts the proposed IBD with current algorithms. The suggested approach provides great results for identifying abnormal behaviours, according to the given table. In a similar manner, it also increases the wrong detection.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: 25 July 2023 Revised: 12 September 2023 Accepted: 30 September 2023

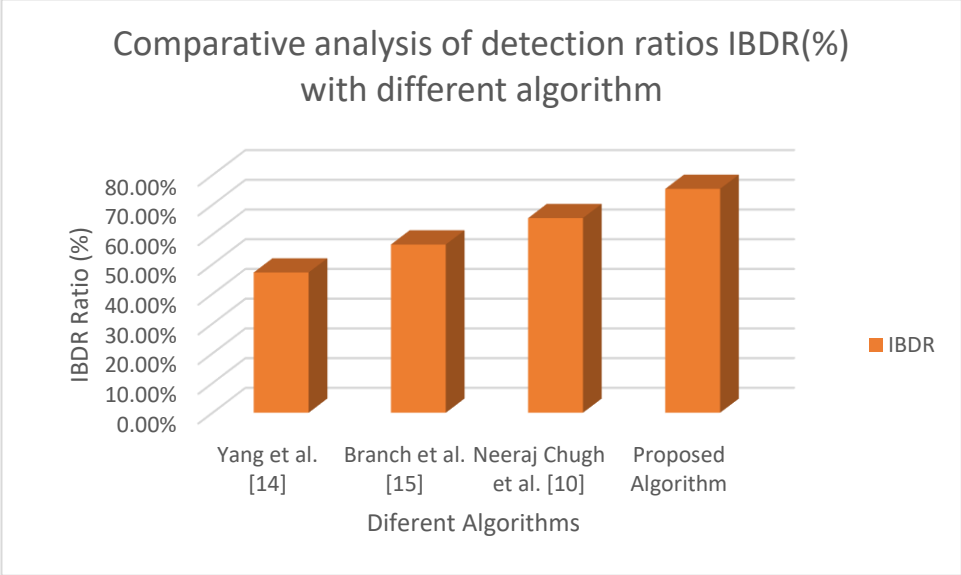

Figure 6: Comparative detection ratio analysis using different algorithms with 500 nodes

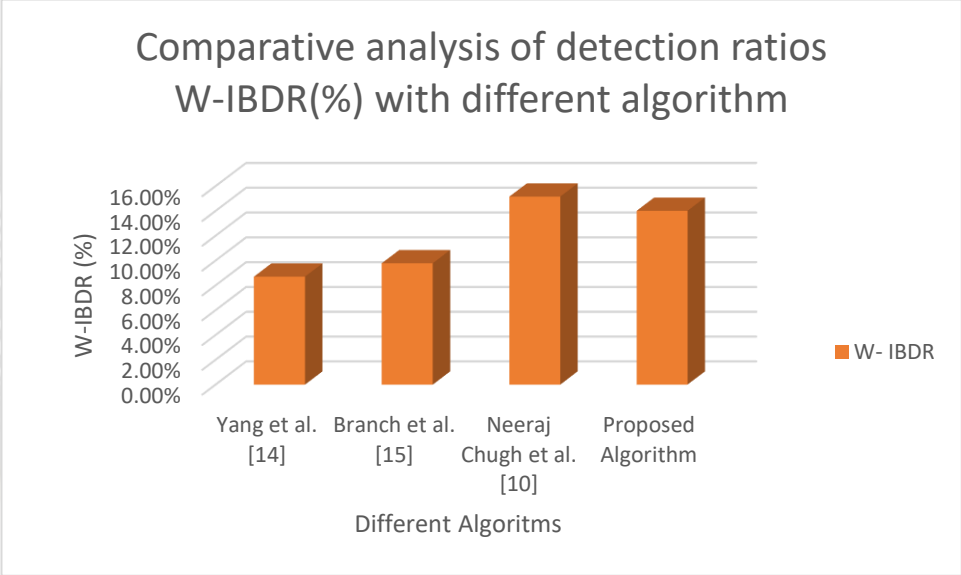

Figure 7: Comparative wrong detection ratio analysis using different algorithms with 500 nodes

7. Conclusion

The proposed Irregularity Behaviour Detection - Ad-hoc On-demand Distance Vector (IBD -AODV) excellently finds the irregular behaviour device in the network. By using trust value, it finds the irregular behaviour of the device. This trust value includes the energy level of the device, the device's network performance, and the position of the device in the network. IBD continuously checks each device's true value to determine which device is available within the group header radio transmission range. The above processes has additional algorithms, It's increase the overhead, so this algorithm gives a little bit more end-to-end time delay (EETD). This proposed algorithm improve device trust. In addition, this algorithm does not have the facility to prevent data change or theft during communication. This result gives a moderate packet delivery ratio. At the final Irregularity Behaviour Detection (IBD), IBD is used to form the trusted device's group for effective communication with less security.

Future Enhancement

This research work does not primarily focus on time complexity, data theft, and data change, the author's previous work has successfully addressed the issue of time complexity. In the current research, a solution has been found for end-to-end time delay through the proposed algorithm, Irregularity Behaviour Detection - Ad-hoc On-demand Distance Vector (IBD-AODV), which effectively handles this aspect. However, it is important to note that the algorithm does not offer protection against data alteration or theft.

Therefore, future efforts will concentrate on addressing security issues. This can be achieved by either incorporating security-related algorithms or developing new procedures specifically designed for security concerns. Consequently, this research serves as an initial stage for addressing and mitigating security issues. Once the security solutions are developed, all the algorithms will be integrated into a Machine Learning algorithm. During this phase, unsupervised learning techniques will be utilized to identify the most suitable solution for each specific situation.

In the future work, the research will employ a trusted device's group for encryption and decryption purposes, further enhancing the security measures implemented.

References

[1]. Neeraj Chugh, Geetam Singh Tomar, Robin Singh Bhadoria and Neetesh Saxena , "A Novel Anomaly Behavior Detection Scheme for Mobile Ad Hoc Networks", Electronics 2021, 10, 1635. https://doi.org/10.3390/electronics10141635.

[2]. Yang, J.; Wang, Y.L. A New Outlier Detection Algorithms Based on Markov Chain. Adv. Mater. Res. 2011, 366, 456–459.

[3]. Branch, J.W.; Giannella, C.; Szymanski, B.;Wolff, R.; Kargupta, H. In-Network Outlier Detection inWireless Sensor Networks. Knowl. Inf. Syst. 2013, 34, 23–54.

[4]. Krishnamachari, B.; Iyengar, S. Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection inWireless Sensor Networks. IEEE Trans. Comput. 2004, 53, 241–250.

[5]. Martincic, F.; Schwiebert, L. Distributed Event Detection in Sensor Networks. In Proceedings of the 2006 International Conference on Systems and Networks Communications (ICSNC'06), Tahiti, French Polynesia, 29 October–3 November 2006; p. 43.

[6]. Jurdak, R.; Wang, X.R.; Obst, O.; Valencia, P. Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies. In Intelligence-Based Systems Engineering; Tolk, A., Jain, L.C., Eds.; Intelligent Systems Reference Library; Springer: Berlin/Heidelberg, Germany, 2011; Volume 10, pp. 309–325. ISBN 978-3-642-17930-3.

[7]. Zhang, Y.; Meratnia, N.; Havinga, P. Outlier Detection Techniques for Wireless Sensor Networks: A Survey. IEEE Commun. Surv. Tutorials 2010, 12, 159–170.

[8]. Yang, J.; Wang, Y.L. A New Outlier Detection Algorithms Based on Markov Chain. Adv. Mater. Res. 2011, 366, 456–459.

[9]. Breunig, M.M.; Kriegel, H.-P.; Ng, R.T.; Sander, J. LOF: Identifying Density-Based Local Outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 15–18 May 2000; p. 12.

[10]. Koufakou, A.; Georgiopoulos, M. A Fast Outlier Detection Strategy for Distributed High-Dimensional Data Sets with Mixed Attributes. Data Min. Knowl. Disc. 2010, 20, 259–289.

[11]. Jain, A.K.; Murty, M.N.; Flynn, P.J. Data Clustering: A Review. ACM Comput. Surv. 1999, 31, 264–323.

[12]. Hawkins, D.M. Identification of Outliers; Chapman and Hall: London, UK, 1980; Volume 11.

[13]. Knorr, E.M.; Ng, R.T. Algorithms for Mining Distance-Based Outliers in Large Datasets; University of British Columbia: Vancouver, BC, Canada, 1998; Volume 98, pp. 392–403.

[14]. Ramaswamy, S.; Rastogi, R.; Shim, K. Efficient Algorithms for Mining Outliers from Large Data Sets. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, TX, USA, 15–18 May 2000; pp. 427–438.

[15]. Branch, J.W.; Giannella, C.; Szymanski, B.;Wolff, R.; Kargupta, H. In-Network Outlier Detection inWireless Sensor Networks. Knowl. Inf. Syst. 2013, 34, 23–54.

[16]. Imani, M. A Novel Approach to Combine Misuse Detection and Anomaly Detection Using POMDP in Mobile Ad-Hoc Networks. Int. J. Inf. Electron. Eng. 2015, 5.

[17]. Rammohan, S.R. Anomaly Detection in Mobile Ad Hoc Networks(MANET) Using C4.5 Clustering Algorithm. Int. J. Inf. Technol. Manag. Inf. Syst. 2015, 1–10.

[18]. Khan, M.S.; Midi, D.; Khan, M.I.; Javaid, N.; Bertino, E. Isolating Misbehaving Nodes in MANETs with an Adaptive Trust Threshold Strategy. Mobile Netw. Appl. 2017, 22, 493–509.

[19]. Prasanna Lakshmi, G.S.; Patil, S.B.; Patil, P. Anomaly Detection in MANET Using Zone Based AODV Routing Protocol. In Advanced Informatics for Computing Research; Luhach, A.K., Singh, D., Hsiung, P.-A., Hawari, K.B.G., Lingras, P., Singh, P.K., Eds.; Communications in Computer and Information Science; Springer: Singapore, 2019; Volume 956, pp. 454–468. ISBN 9789811331428.

[20]. Jabbar Qasim, N.; Majeed Mohammed, S.; Sami Sosa, A.; Albarazanchi, I. Reactive Protocols for Unified User Profiling for Anomaly Detection in Mobile Ad Hoc Networks. Period. Eng. Nat. Sci. 2019, 7, 843.

[21]. Gomathy, V.; Padhy, N.; Samanta, D.; Sivaram, M.; Jain, V.; Amiri, I.S. Malicious Node Detection Using Heterogeneous Cluster Based Secure Routing Protocol (HCBS) in Wireless Adhoc Sensor Networks. J. Ambient Intell. Hum. Comput. 2020, 11, 4995–5001.

[22]. Narayanan, A.E.; Devi, R.; Jayakumar, D.A.V. An Energy Efficient Cluster Head Selection For Fault Tolerant Routing in MANET. Int. J. Eng. Technol. 2013, 5, 9.
[23]. Venkanna, U.; Agarwal, J.K.; Velusamy, R.L. A Cooperative Routing for MANET Based on Distributed Trust and Energy Management. Wireless Pers. Commun. 2015, 81, 961–979.
[24]. Shan, A.; Fan, X.;Wu, C.; Zhang, X.; Fan, S. Quantitative Study on the Impact of Energy Consumption Based Dynamic Selfishness in MANETs. Sensors 2021, 21, 716.
[25]. Krishnan, C.; Gomathi, S.; Anusha Bamini, A.M. High Energy Efficient Lifetime Management System and Trust Management Framework for Manet Using Self-Configurable Cluster Mechanism. Peer-to-Peer Netw. Appl. 2021, 14, 1229–1241.