Journal of Theoretical and Applied Information Technology
15th May 2023. Vol.101. No 9
© 2023 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MOBILITY PREDICTION-BASED SOURCE ANONYMITY ROUTING PROTOCOL (MPSARP) FOR SOURCE LOCATION PRIVACY USING NS2 TECHNIQUES

CHINNU MARY GEORGE[1*], DIVYA SHARMA[2], REEJA S R[3]

[1*] Research Scholar ,Dayananda Sagar University, Bangalore, India

[2]Assistant Professor, Dayananda Sagar University, Bangalore, India

[3]Professor, VIT-AP University, India

1*Corresponding Author : gchinnu2@gmail.com

ABSTRACT

According to information and technology, the three most crucial criteria for success are the three most essential factors in safeguarding privacy in the twenty-first century. As a result, should keep a close check on all of the vast organizations that are watching — companies like Google, Twitter, Facebook, AT&T, and Verizon — making sure they aren't spying on. Every one of these businesses has recently added location-based services to their product or service offerings (or is doing so). Even though I don't reside in a vast geographical area, Twitter can now know what city I'm in and what neighborhood I'm in. Today, consumers face the reality of walking about with a beacon that constantly transmits information about their location to a central server. While capable of broadcasting exact details of our places and movements, cell phones are not the only gadgets that can do so.To address these problems, the study suggested MPSARP ensure location privacy across a wireless network (Mobility prediction-based source anonymity routing protocol). Our proposal is for an Unspecified, efficient routing and location-based system that offers good anonymity protection at a reasonable cost while maintaining excellent performance (MPSARP). By dynamically partitioning a network arena into diverse zones and arbitrarily picking nodes inside zones to serve as intermediary relay nodes, this approach provides a nontraceable unspecified route that is not traceable by the user, resulting in a nontraceable unknown way that is not traceable by the user. The process of simulation is accomplished using NS2 and the performance outperforms the existing techniques.

Keywords: *Mobility, Source Location Privacy, Notify,Piggyback,Routing, Packet Deliver Ratio, Speed, Flows, Delay, Unknown Neighboring Balance.*

1. INTRODUCTION

As technology progresses, sophisticated navigation systems are becoming more common in modern automobiles and laptop computers running software namelygoogle and the correlated apps of search engines, likely Google Maps. Social networks utilize location monitoring as a component of their service (for example, the 'friend finding' tool) or give contextual advertising to their users [1-5]. Although the fact is that almost every handheld gadgets user has turned accustomed to functionality that relies on GPS and position mapping to work, this is not the case [6, 7]. Users of Uber and Lyft, for example, have grown accustomed to the driver knowing where they are and when they would arrive to offer a service [8-10]. Users have become so used to this level of simplicity and it has become second nature for them to deal with the service.. People looking for restaurants or meal delivery services might also benefit from the resources on this page [11, 12]. According to their own words, retail behemoths like Amazon utilises location services to supply and enhance their services [13].

"Voice services, our Maps app, and Find r Device and checking the performance and accuracy of our location services," they explain [14-16]. Location services are also used by Amazon to "deliver and improve our services, such as voice services, the Maps app, and Find r Device," and "track the performance and accuracy of our location services." "We employ location services to check the performance and accuracy of our location services," according to the company. This includes information such as the availability of Amazon Echo devices [17]. Various devices, such as Google's Alexa assistant, utilize location services. In reality, the average consumer will have a hard time finding a "smart" product that does not employ location service. The provision of location-based services is not a challenging task in and of itself. Concerns should be addressed regarding the data collected and the organizations that collect and retain the data. Some people are concerned about data misuse and privacy violations, which they feel will occur due to this issue [18]. Users of social networking sites have begun to express dissatisfaction with the excessive amount of advertising they are exposed to, resulting in the growth of contextual advertising. Location-based services have the potential to enhance almost every area of our lives [19-25].

Furthermore, because numerous devices utilize this type of data, it is critical to separate our everyday activities carefully — keeping even one device active that has this type of access could have a significant impact [26].

To overcomethis issue, the paper proposed MPSARP (Mobility prediction-based source anonymity routing protocol) to ensure location privacy over the WSN. To supply high secrecy security with low fetches, we offer a Mysterious Location-based and Proficient Steering convention (MPSARP). MPSARP powerfully divides a regionfield into areas and arbitrarily chooses hubs in the areas as the access points of the road hand-off hubs, which shape into an untraceable mysterious node. A data sender or forwarder separates the structured field into two zones in each round of steps to isolate itself from the objective. Each game has a point that selects a hub between the other zone as a new transfer hub at random and utilises the Greedy Perimeter Stateless Directing (GPSR) algorithm to convey the data to it. The data is broadcast to k hubs inside the goal zone in the last stage, giving the goal k-anonymity. In addition, MPSARP includes a mechanism for stowing the information initiator among a few initiators to increase the source's namelessness guarantee. MPSARP is also resistant to timing and intersection attacks.

The following sections make up the whole document: Section 2 describes the related work with performance, and Section 3 elucidates the development of a model for MPSARP architecture that describes the work with version. Section 4 describes the proposed work with the performance of the work, which represents the results and analysis of the proposed work with associated work performance. And the development structure for the suggested MPSARP architecture, which is outlined in Section 5, the final section brings the project to a close.

In this research, we propose a (Mobility prediction-based source anonymity routing protocol for UASNs based on mobility prediction. Indeed, by considering a realistic, physically inspired mobility model, our protocol succeeds to forward every generated data packet through one single best path without the need to exchange notification messages, thanks to the mobility prediction module. Simulation results show that our protocol achieves a high packet delivery ratio, high energy efficiency, and reduced end-to-end delay.

2. RELATED WORK

2.1 SAL-SAODV

MANETs based on fog computing are a new mobile ad-hoc network paradigm that combines the benefits of mobility with the benefits of fog computing in a single network. The ad hoc on-demand distance vector (AODV) routing protocol is a classic routing system. It is widely utilized in fog-based MANETs as an alternative to traditional routing methods. The two most essential components of AODV's research field are how to improve transmission performance while also increasing security. On the other hand, it appears that cooperative energy efficiency and security research is a topic that is rarely discussed. The fog-based MANET causes an increase in the number of security needs and technical characteristics that are very diverse and moveable. To simplify the complexity of the SAODV and boost the protocol's energy efficiency, a cyclic redundancy check, rather than a digital signature, is used, as well as a random delayed sending mechanism, to ensure that packets are not tampered with.

In comparison to the SAODV protocol, the SAL-SAODV protocol consumes roughly 35 percent less energy and has a BPUE of nearly 60 percent higher, according to simulation results. The solutions already in use for boosting energy efficiency and information tamper-proofing could benefit a range of various AODV protocols. It's important to note that the random delayed sending strategy used in this implementation will increase end-to-end latency, which will be explored further below. As a result, the SAL-SAODV protocol is appropriate when the latency is not a concern but substantial amounts of security are [28-310.

Objectives:

- To develop a model is for an Unspecified, efficient routing and location-based system that offers good anonymity protection at a reasonable cost while maintaining excellent performance (MPSARP)
- By dynamically partitioning a network arena into diverse zones and arbitrarily picking nodes inside zones to serve as intermediary relay nodes, this approach provides a non-traceable unspecified route that is not traceable by the user
- The process of simulation is accomplished using NS2 and the performance outperforms the existing techniques

2.2 ALERT

The field of mobile ad hoc networks (MANETs) has seen a rush of activity over the last two decades, with most of the effort being directed toward military, disaster relief, and law enforcement applications. Over the past few years, the proliferation of compact and inexpensive GPS receivers, which has been facilitated partly by the trend toward incorporating position-sensing capabilities into personal mobile devices, has increased the accessibility of location data. The evolution of such location-based operations to MANETs is a logical next step in developing the technology. The outcome of this is that we now have what is known as "location-based MANETS." It is critical for the effective operation of devices in a MANET that they have access to location information. The communication paradigm, which is based on instantaneous node position rather than permanent or semi-permanent characteristics, pseudonyms, or addresses is one of the most distinguishing elements of the proposed location-based MANET ecosystem. To put it another way, rather than the other way around, a node (A) makes a connection decision depending on the specific position of another node (B) at the moment of the decision. A physical MANET map may be constructed if node position information is sufficiently detailed, and node positions, rather than persistent node IDs, can be used to identify nodes in the network instead of network addresses. Node IDs are not nearly as relevant as node locations in specific applications, namely law execution, military,and search-and-rescue operations, and are discouraged. Several traits can be found in all significant settings.

First and foremost, understanding node position is critical; understanding physical topology, rather than logical or relative topology, allows for the avoidance of needless communication and the concentration of attention on nodes inside a specific area of the network. Second, crucial settings must be prepared to deal with data breaches and other security and privacy issues. Security threats could propagate malicious routing information, or the flow of legal routing information could be disrupted by negative routing information. On the other hand, privacy attacks are designed to track nodes as they traverse through the network. In risky environments, such as those seen in the military and law enforcement, node identities must remain hidden. Whenever transmission is being observed by antagonistic organizations,which is not a members of the MANET, this is referred to as "hostile monitoring." Let's consider that genuine MANET node may not trust one another (e.g., because of a hypothetical node hack). It becomes even more critical to conceal node identities in real-world MANET environments.

Moreover, in this environment, node motions are automatically masked, making it impossible (or at the very least extremely difficult) to monitor a node, even if the node's identity is known. In civilian settings, apprehensive and unreceptive MANET environments are rare. However, they do exist in the military and law enforcement realm, necessitating the need for advanced security and privacy safeguards [31-35].

Throughout this research, we will study what it takes to offer safe communication while maintaining privacy in hostile and suspicious MANET environments. With the Anonymous Location-Aided Routing in MANETs (ALERT) protocol, which we designed and implemented, we illustrate how significant privacy and security characteristics can be achieved while maintaining acceptable speed. As used in this context, inconspicuousness and confrontation to tracking of nodes are considered to be privacy. Security, on the other hand, is comprised of two components: node/origin authentication as well as location integrity. Our security and privacy qualities appear to be at odds with one another, but we demonstrate how advanced cryptographic techniques can be utilized to bring them together.

3. PROPOSED MPSARP MODEL ARCHITECTURE

Unlike other routing protocols, MPSARP has a vibrant and volatile routing path consisting of several transitional relay nodes that the protocol determines dynamically. As seen in the upper section of Figure 1, we divide a given place horizontally into two zones, P1 and P2, which are labeled as such in the lower portion of Figure 1. After that, we divide zone P1 vertically into two subzones, Q1 and Q2, respectively. Then, we divide zone Q2 into two zones using a technique known as horizontal partitioning. Instead of dividing the minor area all at once, the zone partitioning method utilized in this approach divides it in alternating horizontal and vertical directions.

The phrase "hierarchical zone partitioning" is used to describe this type of partitioning in further depth. In each phase of the routing process, MPSARP selects a node in the subdivided zone to act as an intermediary relay node (i.e., data forwarder), resulting in an impulsive routing path for a message in real-time, according to the routing protocol. The letter ZD stands for the destination zone, which comprises k nodes and contains the letter D. The value of k must be positive to govern the level of anonymity protection provided to the destination. As shown in Figure 1, MPSARP routing is distinguished by the zone division in which each data source or forwarder exists to dispersed itself and the ZD into two zones. The temporary destination (TD) is chosen in the opposite zone. The GPSR routing mechanism sends data from that node to the node neighbouring to the interim endpoint. The network protocol (RF) marked this node as a random forwarder. Data is broadcast to k nodes in ZD during the last step, ensuring that the data is k-anonymous when it reaches its final destination.

The data transmission zone is partitioned into two segments that are further into two sub-regions. The partitioning process with horizontal and vertical partition is indicated as hierarchical zone partition. The data transmission is initiated across the partitioned region, and control is utilized to protect the anonymity of the destination. If data reside in two-zone, it is determined as a temporary destination. An effective routing algorithm transmits the data across the diverse zone to a distinct region. The developed routing approach attains effective transmission. When the transmission zone has n number of nodes to reach the destination D, that is determined as ZD. The control degree is governed using n and ALERT routing partitions the zone segregating the site into the cell that facilitates the data transmission. The positions opted in this transmission are temporary destinations (TD).

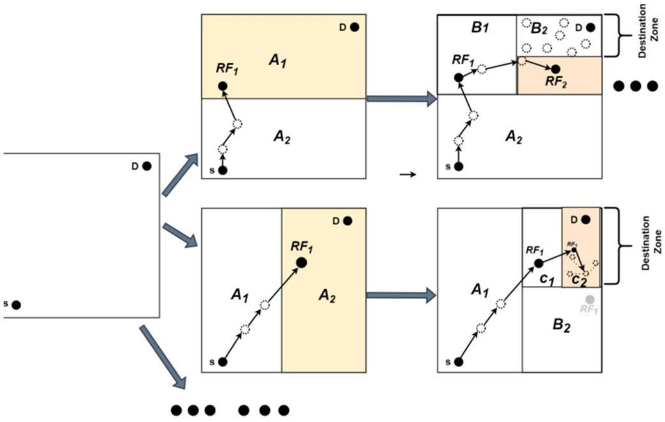

Figure 1 Zone Partition Steps

The above figure depicts two paths that are possible for transmission of data in ALERT that is initiated by source S to sender D.There are plenty of additional options. Data source S segregates the space horizontally into two equal-size zones, A_1 and A_2, to split S and ZD in the full routing flow. We use Z_D instead of D because we don't want D to be exposed. S then chooses the initialtransitoryendpoint, TD1, in zone A_1, where Z_D is located at random. After that, S uses GPSR to deliver pkt to TD_1. Several relays send the Packet until it reaches a node that can't identify a neighbor closer to TD_1. The RF_1 (random-forwarder) node is the name given to this node. When RF_1 is pkt, it splits region A_1 vertically into sections B_1 and B_2, thereby dividing ZD and itself into two zones. Then, at random, RF_1 selects the next provisional destination, TD2, and transmits a packet to TD2 through GPSR. When the packets arrive at their destination, the destination sends a confirmation to the source to ensure delivery. The packages will be resent if the source does not get confirmation within a certain period of time.

When RF_1 gets pkt, it divides region A_1 vertically into areas B_1 and B_2, separating Z_D and itself into two zones. Then RF1 chooses the next temporary destination, TD_2, at random and sends pkt to TD_2 using GPSR. This procedure is continued until a packet receiver locates itself in ZD, i.e., a partitioned zone with k nodes is ZD. The pkt is then broadcast to the k nodes by the node. When the destination receives the packets, it sends a confirmation to the source to assure delivery. If the source does not get the confirmation within a specific time, the packages will be resent.ALERT helps achieve anonymity by limiting a node's visibility to just its neighbors and using the same initial and forwarded messages. This makes determining whether a node is a source or a forwarding node challenging for an intruder. We also suggest a lightweight approach termed "notify and go" to augment the source nodes' anonymity protection. Its central concept is to have several nodes send out packets simultaneously as S to disguise the source packet, among many others.

Allowing a large number of nodes to send packets simultaneously as S is one of the protocol's fundamental principles since it will enable the source packet to be hidden amid a vast number of other packages. The phrase "notify and go" can be broken down into two parts: "notify" and "go." During the first "alert" phase, a data transmission notice is piggybacked on periodic update packets, allowing S to inform its neighbors that it is about to send out a data transmission without them knowing. The letters t and t0 stand for two different random back-off periods stored within the same Packet. When S and its neighbors enter the second "go" phase, they must first wait a specific time [0, 0, t, t+t0] before sending messages.

To keep up with the amount of traffic generated by the data source, S's neighbors just need to develop a few bytes of random data. The value of t must have no bearing on transmission latency; as a result, it should be kept as low as possible. The length of time zero (t0) may result in interference since many packets are sent out simultaneously, while the duration of time zero (t0) may result in a significant transmission delay. To prevent any intruder from differentiating S, the time interval t0 should be long enough to minimize interference while balancing the delay between S and S's nearest neighbor. This camouflage helps raise the level of privacy protection provided to S, where S is the number of neighbors it has on either side, by using -anonymity. As a result, an attacker won't be able to use traffic analysis to find S.

4. RESULT AND DISCUSSION

Simulation parameter:

Parameter	**Value**
Simulator	NS-2.29
Node Count	Fifty to two hundred and fifty
Topology	Random
Propagation Technique	Two Ray Ground
Physical Technique	Wirelessly
Antenna Technique	Omni antenna
Size of the Queue	Fifty
Type of the Traffic	UDP, CBR
Routing Algorithm	MPSARP
Packet size	500 bytes
Rounds	200 sec
Mobility of nodes	5,10,15,20 and 25

This section shows the quantitative value obtained by using the MPSARP method for estimating. The NS-2 emulator and hierarchical structure are used to simulate the situation. Here, performance metrics like beacon overhead, delay, packet delivery rate, energy and the unknown neighboring ration were measured. Here, the proposed technique is associated with Alert and SAL-SAODVTechniques input parameter nodes and mobility. A node represents the number of connected users on the WSN; speed has been concentrated due to heavy load. Flows represent the source and destination pairs in the environment. The obtained performance metrics differ reliant on the count of nodes and flows present. Table 1 depicts the beacon that floats above the flow patterns. The beacon frame is one of the administration frames used in IEEE 802.11-based wireless local area networks.

Table 1 Beacon Overheads Of The Flows

	SAL-SAODV	MPSARP	ALERT
15	672	623	675
20	896	856	901
25	1334	1297	1342
30	2348	2302	2356
35	3415	3367	3421
40	3862	3792	3870

It is organized hierarchically and comprises all of the information related to the network's activity. Beacon frames are sent out regularly to confirm the occurrence of a wireless LAN while also keeping the adherents of the service in sync with one another.

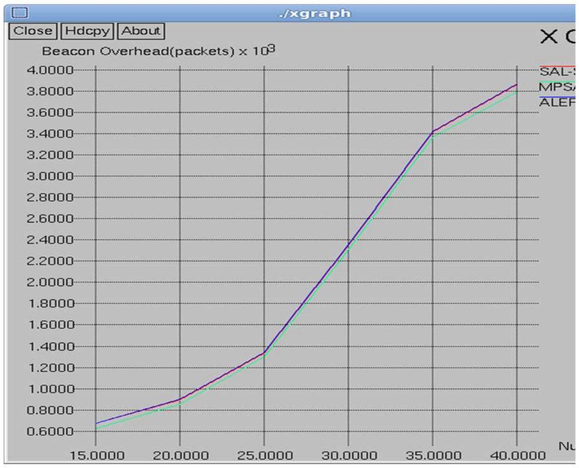

Figure 2 Analysis Of Beacon Overheads Of The Flows

In an infrastructure basic service set, the access point (AP) transmits beacon frames to the network as part of the basic service set (BSS). Figure 2 compares the beacon overheads of the proposed model to another existing model

Table 2 Beacon Overheads Of The Speed

	SAL-SAODV	MPSARP	ALERT
5	0.09	0.07	1.0
10	0.95	0.12	1.3
15	1.3	0.92	1.4
20	1.1	1.0	1.6
25	1.5	1.4	1.7
30	1.6	1.5	1.9

In this, the proposed model got significantly less beacon overhead of 3792 when compared with the other two techniques. Beacon overheads of speed have been represented in table 2. It achieves the minimum overheads of 1.5 and has been evaluated in figure 3

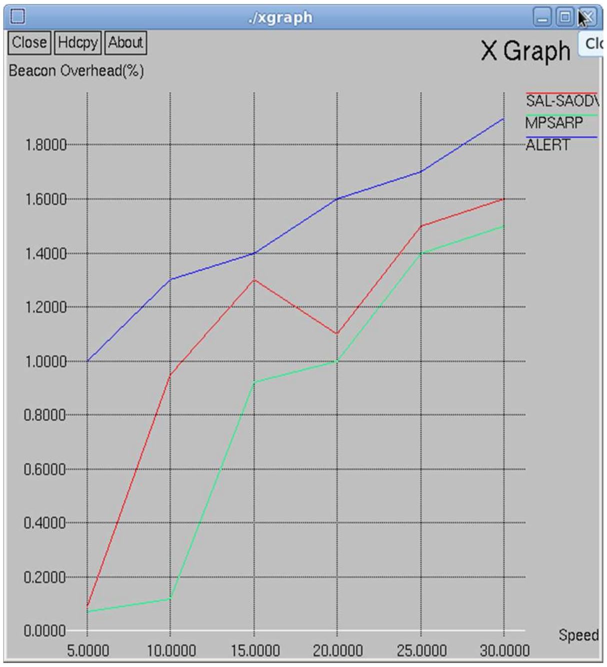

Figure 3 Analysis Of Beacon Overheads Of The Speed

Table 3 compares the PDR of flows encountered MPSARP model. The total number of nodes is 40 used for simulation. Delivery ratio in node 15, 20, 25, 30, 35 and 40 is 99.93,95.68,93.69,91.20,87.49 and 85.02respectively and it has been described on the figure 4.

Table 3 Packet Delivery Ratio Of Flows

	SAL-SAODV	MPSARP	ALERT
15	99.83	99.93	99.87
20	94.68	95.68	93.27
25	92.69	93.69	91.09
30	89.20	91.20	87.35
35	85.49	87.49	82.67
40	82.02	85.02	80.98

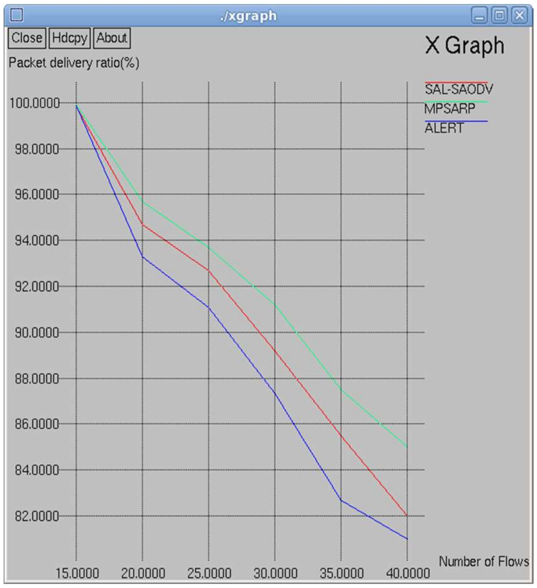

Figure 4 Packet Delivery Ratio Of Flows

Table 4 compares the PDR of speed encountered MPSARP model. The total number of nodes is 30 used for simulation. The delivery ratio in nodes 5, 10, 15, 20, 25, and 30 is 99.92, 95.23, 93.45, 90.95, 87.63 and, 83.48respectively, and it has been described in figure 5

Table 4 Packet Delivery Ratio Of The Speed

	SAL-SAODV	MPSARP	ALERT
5	99.92	99.92	99.87
10	94.23	95.23	93.27
15	92.45	93.45	91.09
20	89.95	90.95	87.35
25	85.63	87.63	82.67
30	81.48	83.48	80.98

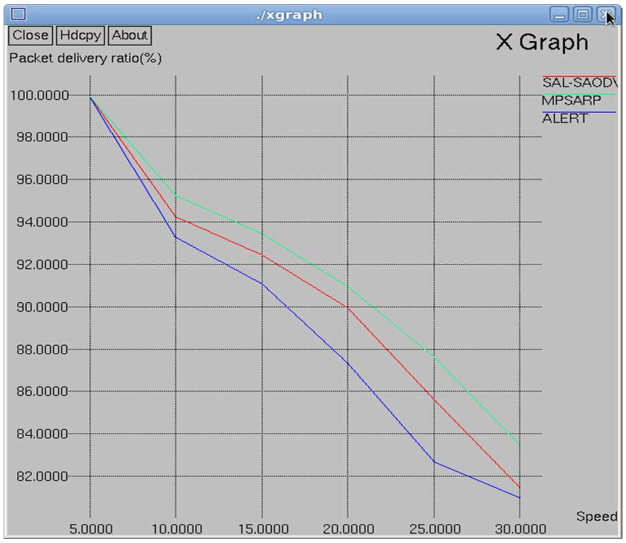

Figure 5 Packet Delivery Ratio Of The Speed

Table 5indicates the comparison of delay encountered, and a total count of nodes is 25 utilised for replication. Delay in node 0, 5, 10, 15, 20, 25 is0.012,0.02,0.03,0.04 and 0.08 respectively. Figure 6 represents the speed delay of the proposed work

Table 5 Speed-Delay

	SAL-SAODV	MPSARP	ALERT
5	0.018	0.012	0.020
10	0.10	0.02	0.14
15	0.12	0.03	0.19
20	0.16	0.04	0.21
25	0.19	0.08	0.27

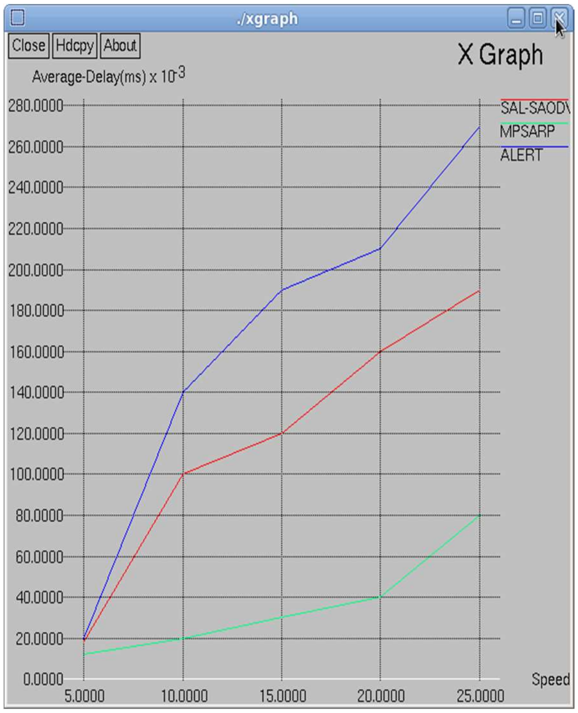

Figure 6 Comparison Of Speed-Delay

. Table 6 shows the comparison of energy encountered, and a total number of nodes is 25 used for simulation. Energy consumption in nodes 5, 10, 15, 20, 25 is 11.48, 16.21,22.48, 26.12 and 31.58respectively, it has been described in figure 7.

Table 6 Speed-Energy

	SAL-SAODV	MPSARP	ALERT
5	8.65	11.48	7.65
10	13.93	16.21	12.93
15	18.30	22.48	17.30
20	24.48	26.12	23.48
25	28.17	31.58	27.17

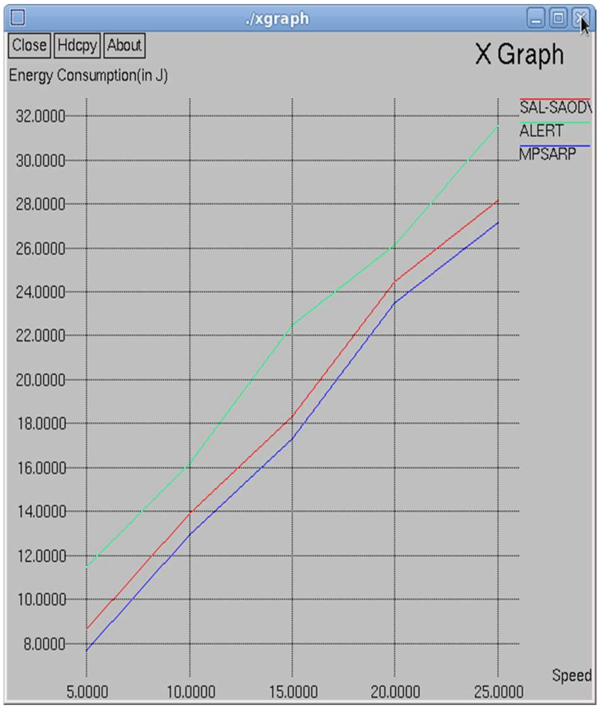

Figure 7 Comparison Of Speed-Energy

Table 7 compares unknown neighboring ratios encountered, and the total number of nodes is 25 used for simulation. Unknown factor in node 0, 5, 10, 15, 20, 25 is 0.00,0.01,0.02, 0.06 and 0. 07respectively.Figure 8 represents the unknown neighboring ratio of the proposed work with the existing analysis.

Table 7 Speed- Unknown Neighbouring Ratio

	SAL-SAODV	MPSARP	ALERT
5	0.01	0.00	0.03
10	0.02	0.01	0.07
15	0.03	0.02	0.09
20	0.07	0.06	0.12
25	0.09	0.07	0.19

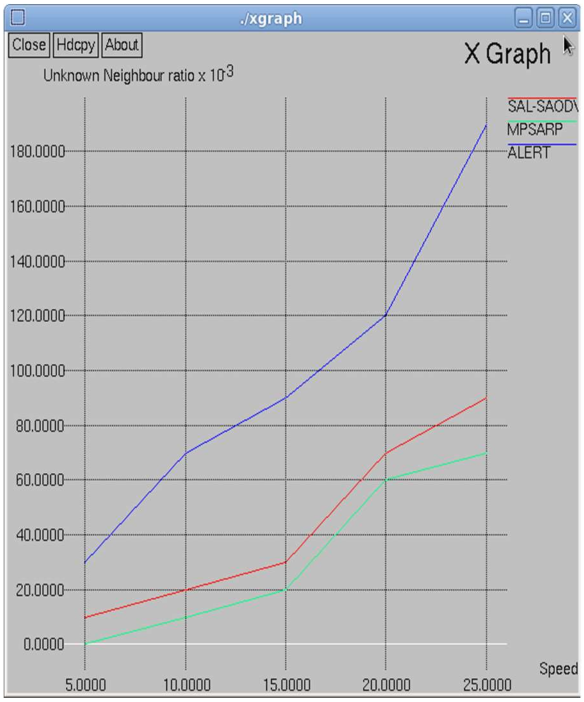

Figure Analysis Of Speed- Unknown Neighbouring Ratio

Our proposed model has been compared with existing techniques by measuring different performance metrics like high packet delivery ratio, high energy efficiency, and reduced end-to-end delay.

6. CONCLUSION

Previous anonymous routing systems were costly to achieve anonymity and source location privacy, dependent on either replicated traffic or encryption scheme is attained by hop-by-hop. Unknown routing solutions are now significantly more affordable. Furthermore, due to restrictions in the way they operate, several protocols cannot offer total anonymity defence at the source and destination. MPSARP provides anonymity defence for sources, goals, and route information and charges a minimal charge with the mobility prediction and piggybacks Packet. A dynamic hierarchical zone splitting method is used in conjunction with arbitrary relay node collections to make it challenging for an impostor to identify the two endpoints and noderoutes. When MPSARP is used, a packet containing the source and destination zones rather than their locations is delivered to protect the source and destination's anonymity during transmission. Because the data initiator/receiver is buried among many data initiators/receivers in MPSARP, the origin and destination of the data are protected even more. MPSARP also gives users a highly effective means of defending themselves against overlapping attacks. MPSARP's capacity to defend against time-based attacks is also being investigated. Compared to other anonymity algorithms, the outcome depicts that MPSARP can provide strong anonymity defence at a minimal cost. It can also match the baseline GPSR technique routing efficiency, which is remarkable. Because the MPSARP anonymity routing technique, like all other anonymity routing algorithms, is not entirely impenetrable to all attackers, MPSARP will be strengthened to prevent future attackers who will be more powerful and aggressive in their approach. A complete theoretical and simulated environment demonstration of the technology will also be presented.

REFERENCES

[1]. Mutalemwa, Lilian C., and Seokjoo Shin. "Comprehensive performance analysis of privacy protection protocols utilizing fake packet injection techniques." *IEEE Access* 8 (2020): 76935-76950.

[2]. Singh, Pranav Kumar, Shivram N. Gowtham, S. Tamilselvan, and Sukumar Nandi. "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs." *Vehicular Communications* 20 (2019): 100183.

[3]. Manjula, Raja, and Raja Datta. "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs." *Pervasive and Mobile Computing* 44 (2018): 58-73.

[4]. He, Yu, Guangjie Han, Hao Wang, James Adu Ansari, and When Zhang. "A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things." *Future Generation Computer Systems* 96 (2019): 438-448.

[5]. H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, ``A probabilistic source location privacy protection scheme in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 68, no. 6, pp. 5917_5927, Jun. 2019

[6]. He, Yan, and Jiageng Chen. "User location privacy protection mechanism for location-based services." *Digital Communications and Networks* (2020).

[7]. Rios, Ruben, and Javier Lopez. "Exploiting context-awareness to enhance source-location privacy in wireless sensor networks." *The Computer Journal* 54, no. 10 (2011): 1603-1615.

[8]. M. Bradbury and A. Jhumka, ``A near-optimal source location privacy scheme for wireless sensor networks," in Proc. IEEE Trust- com/BigDataSE/ICESS, Aug. 2017, pp. 409_416.

[9]. H. Wang, G. Han, W. Zhang, M. Guizani, and S. Chan, ``A probabilistic source location privacy protection scheme in wireless sensor networks," IEEE Trans. Veh. Technol., vol. 68, no. 6, pp. 5917_5927, Jun. 2019.

[10]. Chakraborty, Bodhi, Shekhar Verma, and Krishna Pratap Singh. "Staircase-based differential privacy with branching mechanism for location privacy preservation in wireless sensor networks." *Computers & Security* 77 (2018): 36-48.

[11]. Jian, Ying, Shigang Chen, Zhan Zhang, and Liang Zhang. "A novel scheme for protecting receiver's location privacy in wireless sensor networks." *IEEE Transactions on Wireless Communications* 7, no. 10 (2008): 3769-3779.

[12]. Han, Guangjie, Mengting Xu, Yu He, Jinfang Jiang, James Adu Ansere, and Wenbo Zhang. "A dynamic ring-based routing scheme for source location privacy in wireless sensor networks." *Information Sciences* 504 (2019): 308-323.

[13]. Christopher, V. Bibin, and J. Jasper. "Jellyfish dynamic routing protocol with mobile sink for location privacy and congestion avoidance in wireless sensor networks." *Journal of Systems Architecture* 112 (2021): 101840.

[14]. Rios, Ruben, Jorge Cuellar, and Javier Lopez. "Probabilistic receiver-location privacy protection in wireless sensor networks." *Information Sciences* 321 (2015): 205-223.

[15]. Mahmoud, Mohamed MEA, and Xuemin Shen. "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks." *IEEE Transactions on Parallel and Distributed Systems* 23, no. 10 (2011): 1805-1818.

[16]. Han, Guangjie, Xu Miao, Hao Wang, Mohsen Guizani, and Wenbo Zhang. "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks." IEEE Transactions on Vehicular Technology 68, no. 3 (2019): 2739-2750.

[17]. J. Long, M. Dong, K. Ota, and A. Liu, ``Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks," IEEE Access, vol. 2, pp. 633_651, 2014.

[18]. Wang, Na, Junsong Fu, Jiwen Zeng, and Bharat K. Bhargava. "Source-location privacy full protection in wireless sensor networks." Information Sciences 444 (2018): 105-121

[19]. I. Bouazizi. ARA - The Ant-Colony Based Routing Algorithm for MANETs. In Proc. of ICPPW, 2002.

[20]. D. Chaum, C. O. T. Acm, R. Rivest, and D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24:84–88, 1981.

[21]. T. Chothia and K. Chatzikokolakis. A Survey of Anonymous Peer-to-Peer File-Sharing. In Proc. of NCUS, pages 744–755, 2005.

[22]. Hui Li Jianfeng Ma Xiaoqing Li and Weidong Zhang. An efficient anonymous routing protocol for mobile ad hoc networks. In IAS, pages 287–290, 2009.

[23]. Liu Yang, Markus Jakobsson, and Susanne Wetzel. Discount anonymous on-demand routing for mobile ad hoc networks. Securecomm and Workshops, 2006, pages 1–10, 28 2006-Sept. 1 2006.

[24]. Chansu Yu, Kang G. Shin, and Lubo Song. Link-layer salvaging for making routing progress in mobile ad hoc networks. In MobiHoc ’05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pages 242–254, New York, NY, USA, 2005. ACM.

[25].] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang. Mask: anonymous on-demand routing in mobile ad hoc networks. Wireless Communications, IEEE Transactions on, 5(9):2376–2385, September 2006.

[26]. Bo Zhu, Zhiguo Wan, M.S. Kankanhalli, Feng Bao, and R.H. Deng. Anonymous, secure routing in mobile ad-hoc networks. Local Computer Networks, 2004. 29th Annual IEEE International Conference on, pages 102–108, Nov. 2004.

[27]. C.-C. Chou, D. S. Wei, C.-C. J. Kuo, and K. Naik. An efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc networks. In JSAC, pages 192–203, 2007.

[28]. Mansour, H. S., Mutar, M. H., Aziz, I. A., Mostafa, S. A., Mahdin, H., Abbas, A. H., ... &Jubair, M. A. (2022). Cross-Layer and Energy-Aware AODV Routing Protocol for Flying Ad-hoc Networks. *sustainability*, *14*(15), 8980.

[29]. Zhang, D., Gong, C., Zhang, T., Zhang, J., & Piao, M. (2021). A new algorithm of clustering AODV based on edge computing strategy in IOV. *Wireless Networks*, *27*(4), 2891-2908.

[30]. Nabati, M., Maadani, M., &Pourmina, M. A. (2022). AGEN-AODV: an intelligent energy-aware routing protocol for heterogeneous mobile ad-hoc networks. *Mobile Networks and Applications*, *27*(2), 576-587.

[31]. Gupta, N., Vaisla, K. S., Jain, A., Kumar, A., & Kumar, R. (2022). Performance Analysis of AODV Routing for Wireless Sensor Network in FPGA Hardware. *Comput. Syst. Sci. Eng.*, *40*(3), 1073-1084.

[32]. Al-Shareeda, M. A., & Manickam, S. (2022). Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. *Symmetry*, *14*(8), 1543.

[33]. Bondada, P., Samanta, D., Kaur, M., & Lee, H. N. (2022). Data security-based routing in MANETs using key management mechanism. *Applied Sciences*, *12*(3), 1041.

[34]. Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., &Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. *IEEE Access*, *9*, 120996-121005.

[35]. Kalime, S., & Sagar, K. (2021). A review: secure routing protocols for mobile adhoc networks (MANETs). *Journal of Critical Reviews*, *7*, 8385-8393.