Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

Develop a Mathematical Model to Secure Anonymous Communication in Manet Through Cluster Framework

Swetha M S [1], Kallur V Vijayakumar [2], Muneshwara M S [3], Chethan A S [4], Anand R [5], Shivakumara T [6]

[1,] Department of Information Science and Engineering, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0002-6669-1372] swethams_ise2014@bmsit.in

[2,] Department of Mathematics, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0002-7205-1144] kallurvijayakumar@bmsit.in

[3,] Department of Computer Science and Engineering, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0003-4714-4100] muneshwarams@bmsit.in

[4,] Department of Mathematics, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0002-7002-9349] aschethan@bmsit.in

[5,] Department of Computer Science and Engineering, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0001-5028-8661] anandor@bmsit.in

[6,] Department of Master in Computer Application, BMS Institute of Technology and Management Yelahanka, Bengaluru, India. [0000-0002-5213-0953] shivakumarat@bmsit.in

* Corresponding author's Dr. Swetha M S, Email: swethams_ise2014@bmsit.in

Article History:

Received: *13-05-2024*

Revised: *26-06-2024*

Accepted: *13-07-2024*

Abstract:

Introduction: MANETs employ intricate routing protocols that obscure node identities and routes from external observers, thereby ensuring anonymity and security. However, existing anonymous networking protocols relying on either hop-by-hop encryption or excessive traffic generation incur significant costs and often fail to provide complete anonymity protection for data sources, destinations, and routes due to emerging self-organization and self-reinforcement constraints.

Objectives: To provide robust anonymity assurance at minimal cost, the research work proposes Secure Clustered Location-Based Routing Protocol (SCLBRP), The research work is evaluated for the network model is considered with performance parameter Energy and Network life time.

Methods: To provide robust anonymity assurance at minimal cost, the research work proposes Secure Clustered Location-Based Routing Protocol (SCLBRP), in MANET utilizing optimal partitioning and cluster model. In SCLBRP First divides the network into zones using the Optimal Zone Partitioning (OZP) algorithm and cluster trust calculation Optimal Trust Inference Algorithm (OTIA).

Results: The evaluation of the network model is considered with performance parameter Energy and Network life time. The proposed work is compared with the AASR and ALERT protocol with the help of Mathematical equation of energy and network live time. The work is proved that proposed work is giving better performance

Conclusions: The research work focused in proposing a Secure Clustered Location-Based Routing Protocol (SCLBRP) for MANET. The highest trust degree is act as CH in the cluster among multiple mobile nodes. Optimal Trust Inference Algorithm (OTIA) is used to compute the optimal path among multiple paths. Finally, the proposed SCLBRP

protocol is proved with better performance with existing protocol terms of energy and network lifetime.

Keywords: **Mobile ad-hoc network (**MANET), Secure Clustered Location-Based Routing Protocol (SCLBRP), Optimal Zone Partitioning (OZP), Optimal Trust Inference Algorithm (OTIA)

1. Introduction

MANET comprises nodes capable of communicating with each other via wireless mediums. These nodes serve not only as endpoints but also as relays to forward packets to others, independent of any established infrastructure or centralized organization [1]. Ensuring trusted and secure communications in poorly structured environments like battlefields poses significant challenges. Designing routing protocols for such unpredictable conditions in MANETs is particularly daunting due to the mobility and potential failures of nodes [2]. The necessity for fault-tolerant and secure routing protocols has been recognized to address communication in challenging environments, especially amidst damaged nodes, by leveraging network redundancies [3-4].

Security is crucial in adversarial environments where central nodes in the network cannot be consistently trusted, as they may fall into enemy hands and become compromised. Therefore, anonymous communications play a vital role in MANETs under hostile conditions [5], where traditional identifiers and routes are replaced with random numbers or aliases for security purposes. Over the past decade, numerous anonymous routing protocols have been proposed. A notable example is the approach used in on-demand ad hoc routing protocols like AODV and DSR [6]. Anonymous routing protocols ensure secure data transmission by obscuring information compared to other systems [7].

ALERT protocol typically refers to a mechanism used to notify network administrators or users about critical events or issues [8]. The AASR protocol is designed for secure routing in Mobile Ad hoc Networks (MANETs), focusing on adaptability and acknowledgment mechanisms to enhance security [9].

2. Literature Survey

Research is currently focused on enhancing the security and efficiency of anonymous routing algorithms [10]. To address the fundamental requirements for anonymity, a comprehensive literature review was conducted to assess their effectiveness in secure communication. Several innovative approaches to anonymity are highlighted below[11].

Zhang et al. [12] introduced a bio-inspired hybrid trusted routing protocol (B-iHTRP) integrating trusted analysis, physarum autonomic optimization (PAO), and ant colony optimization (ACO). They incorporated cross-layer intelligence into ACO to enhance the security of perceiving ants. Within each zone, proactive maintenance of route tables by intelligent ants facilitated parameter detection. Between zones, responsive scouting ants were deployed to discover routes to destinations while identifying relevant parameters. Furthermore, B-iHTRP utilized PAO to select optimal routes among

those discovered and autonomically optimized local routes across multi-zone communication domains. While the combination of ACO and PAO techniques significantly improved performance, it was noted to be less efficient than Distributed Hash Table (DHT) based routing protocols due to higher energy consumption.

Biswas et al. [12] proposed a solution to detect and mitigate black hole attacks while ensuring secure packet transmission and efficient resource utilization in mobile ad hoc networks (MANETs). Their approach involves assessing the trustworthiness of each node in the network based on parameters such as node mobility, uptime, remaining battery power, etc. Node trust forms the basis for determining the most reliable route for packet transmission. While their method offers commendable performance in terms of throughput, secure routing, and efficient resource management, it does not significantly enhance performance

Due to the inherent complexities of radio transmissions, wireless networks face unique challenges. S. Seys and B. Preneel introduced the ARM (Anonymous Routing Protocol for Mobile Ad-hoc Networks) algorithm. Their research focuses on probability distributions of TTL (Time-to-Live) values and padding probability distributions. The ARM algorithm is designed as a novel anonymous on-demand routing protocol for wireless MANETs, emphasizing its security against node compromise [13].

Leena Jadhav et al. introduced the Reliable DREAM protocol, which outperforms traditional AODV routing. DREAM focuses on analyzing metrics such as Average Packet Delivery Ratio and Mean Route Discovery Delay, while also managing node mobility and sustaining location information. The protocol calculates the expected probability of node movement and minimizes packet flooding by directing packets towards the anticipated destination location. Each node in the network continuously updates and maintains location information for nearby nodes, adapting to the dynamic changes in node positions. The Reliable DREAM protocol significantly enhances routing performance and ensures efficient data delivery in dynamic network environments [14].

Uma R. B. et al. introduced an enhanced DSR (Dynamic Source Routing) algorithm for Mobile Ad hoc Networks (MANETs).[15] This algorithm addresses the issue of excessive flooding of RREQ (Route REQuest) packets, which typically leads to congestion and increased energy consumption in the network. In their approach, when a node receives a RREQ packet, it evaluates its own residual battery power, received signal strength, and speed. Based on this assessment, the node makes a decision whether to forward the RREQ packet or not. This proactive measure helps prevent unnecessary flooding of RREQ packets throughout the network, thereby improving overall system performance.

Gang, Z., Han et al. proposes a hybrid DTN-DSR protocol to satisfy the particular request that applies DTN architecture to the highway environment. It considers the network as a structure of clusters. If there is an effective path from source to destination it uses DSR protocol. Otherwise it uses asynchronous DTN protocol to take custodial transmission [16]

3. Proposed Method

The proposed method Secure Clustered Location-Based Routing Protocol (SCLBRP) as shown in fig-1. In a MANET, the network is composed of cluster head nodes (CHs), mobile nodes (cluster members), and potentially malicious nodes (MNs). CHs play a crucial role in gathering information from mobile nodes. Initially, mobile nodes are scattered randomly throughout the network. Once clusters are formed, the trustworthiness of each node is evaluated using various metrics. Continuous data transfer within the same node can lead to significant energy consumption. The node with the highest trust score is designated as the CH, responsible for collecting data from cluster members and forwarding it towards the destination within the network [17]. This ensures efficient data aggregation and secure transmission in MANET environment.

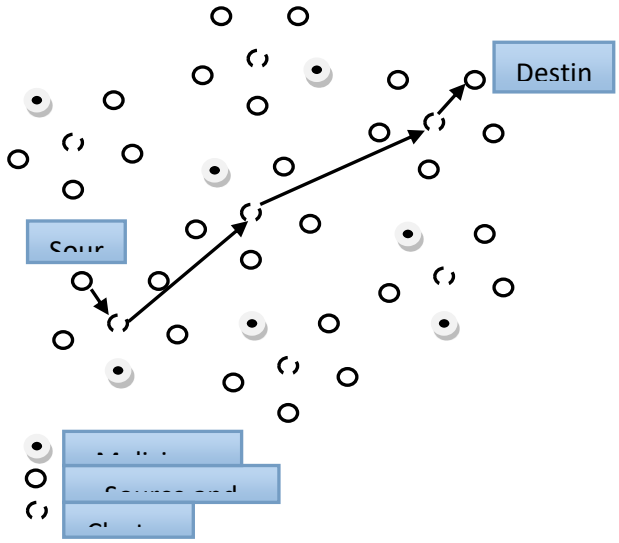

Fig-1 Model of Secure Clustered Location-Based Routing Protocol (SCLBRP)

One straightforward heuristic approach for addressing a stochastic depletion problem is the myopic policy. In this policy, when in state S, one selects a set of activities that maximizes the expected reward earned in the next time-step [18]. This approach focuses on maximizing immediate gains based on current conditions without considering long-term implications or future states.

$$\prod^{g}(S) \in \arg\max_{a \in S_A} E\left[R(S, S_A)\right] \tag{1}$$

To evaluate its effectiveness, we compare the performance of the improved myopic heuristic against an optimal clairvoyant algorithm [19]. The clairvoyant algorithm possesses complete knowledge of the Pt processes beforehand. Since an optimal clairvoyant policy inherently outperforms any other policy, demonstrating performance guarantees relative to this optimal clairvoyant policy suffices. Thus, we aim to assess how closely the improved myopic heuristic approximates the performance of the clairvoyant algorithm in maximizing total rewards over time [19].

$$S_A = \left(\min\left(E_T, RC, L_{nw}, D\right) \cup \max\left(T_{nw}\right) : 0 < t \le T\right) \tag{2}$$

Moving forward, our focus will solely be on optimal policies; whenever we mention an optimal policy or value function, it pertains specifically to the clairvoyant problem. The CH node within the cluster set is chosen based on the sensor node possessing the highest optimal value[21].

$$CH_i = \sum_{i=1}^{n} S_{A_i} \tag{3}$$

Finally, the Brown function [34] used to crosscheck the elected CH node as follows:

$$F(S_A) = \sum_{i=1}^{n} \left(S_{A_i}^2\right)^{\left(S_{A_{i+1}}^2+1\right)} + \left(S_{A_{i+1}}^2\right)^{\left(S_{A_i}^2+1\right)} \tag{4}$$

The lifetime of a sensor node is defined by the maximum number of packets it can transmit to the sink. Since the time required to transmit a single packet is typically very short, it is negligible when analyzing sensor lifetime [22-23]. Furthermore, network connectivity is directly influenced by node density. Hence, defining lifetime based on the percentage of nodes that have ceased functioning offers insights into network longevity that are complementary to metrics based on connectivity and coverage.

$$t_i = \sum_{j=1}^{[p_i]} \lambda^{p_1} \frac{x^{p_1-1} e^{-\lambda\tau}}{\Gamma(p_i)} \tag{5}$$

where p_i represents the maximum number of packets that sensor i can transmit during time τ Then, lifetime of the network as follows:

$$NLT = T\left[\max(t_i) \in \frac{N_a}{N}\right] \tag{6}$$

where N is the number of sensors in the network and N_a is the number of alive nodes. The route cost (RC) between two nodes are defined as follows,

$$RC(n,d) = \sum_{i,j \in (n,\cup,d)} \text{cost}_{i,j} \tag{7}$$

where $\text{cost}_{i,j}$ cost function for a link between nodes i and j. Thus,

$$\text{cost}_{i,j} = E_p + 2\,N\,E_{tx}(n,d) + e^{\frac{1}{E_R^i}} \tag{8}$$

where E_R^i is cost function that takes into consideration the remaining energy of sensors for the energy balance among sensors[24].

The acceleration of an agent is computed by taking total forces from a group of heavier masses and it is based on the law of gravity equation (6) and it is calculated based on the law of motion (7). The velocity of an agent is calculated by taking the fraction of its current velocity adding to its acceleration (8) and next position is calculated by the equation (9). Afterwards, next velocity of an

agent is calculated as a fraction of its current velocity added to its acceleration (Eq. (9)). Then, its next position can be calculated using Eq. (10):

$$F_i^d(t) = \sum_{j \in kbest,\, j \neq i} rand_j G(t) \frac{M_j(t) M_i(t)}{R_{ij} + \varepsilon} \left(x_j^d(t) - x_i^d(t) \right) \tag{9}$$

$$a_i^t(t) = \frac{F_i^d(t)}{M_i(t)} = \sum_{j \in kbest,\, j \neq i} rand_j G(t) \frac{M_j(t)}{R_{ij} + \varepsilon} \left(x_j^d(t) - x_i^d(t) \right) \tag{10}$$

$$V_i^d(t+1) = rand_i \times V_i^d(t) + a_i^d(t) \tag{11}$$

$$X_i^d(t+1) = X_i^d(t) + V_i^d(t+1) \tag{12}$$

where $rand_i$ and $rand_j$ indicates uniformly distributed random number present in the interval [0,1], ε indicate the small value, $R_{ij}(t)$ indicate the Euclidean distance between two agents i and j and it is defined as $||X_i(t)X_j(t)||_2$. The set of first K agents is given as Kbest which include [25] best fitness value and biggest mass. The K indicate the function of time and the initial value is given by $K_{initial}$ value and value will decrease with time. G(t) indicate the gravitational constant and the initial value is given by $G_{initial}$:

$$G(t) = G(G_{initial}, G_{end}, t) \tag{13}$$

For finding the location of the application nodes (AN) are calculated here. Consider the initial energy as $E_j(0)$, the data transmission rate is given by r_j, the distance –independent parameter is given by a_{j1} and the distance-dependent parameter of the j^{th} AN is given by a_{j2}. The lifetime ($l_{ij}(t)$) is given by:

$$l_{ij}(t) = \frac{E_j(0)}{r_j(a_{j1} + a_{j2}\, d_{ij}^n)} \tag{14}$$

Where d_{ij}^n indicate n-order Euclidian distance. The fitness function is given by:

$$f_i(t) = \underset{j \in \{1,\ldots\ldots m\}}{Min} l_{ij}(t) \tag{15}$$

Where number of AN is given by m. If the fitness value is high then the lifetime is high.

Our model undergoes evaluation using the NS2 tool across various network scenarios. Mobile nodes are randomly deployed within a network area of 1500m × 1500m. We explore scenarios comprising 50, 100, 150, 200, and 250 nodes distributed randomly throughout the network

4. Results and Discussion

The proposed method Secure Clustered Location-Based Routing Protocol (SCLBRP) technique is employed on 50, 100, 150, 200 and 250 node network to illustrate its effectiveness, which used to maximize the energy efficient in sensor nodes using Optimal Zone Partitioning (OZP) and Optimal Trust Inference Algorithm (OTIA) our proposed protocol provide better results by minimizing the

parameters energy consumption and maximize network lifetime. The simulation is done with varying number of node.

Table-1: Comparison of existing protocol with proposed SCLBRP with 2 different metrics by varying number of nodes

Count of Nodes	Energy consumption				Network lifetime			
	A	B	C	D	A	B	C	D
50	1	3.10	5.50	4.50	51	1	13	12
100	2	5.80	6.10	5.0	63	32	32	22
150	3	6.10	7.90	6.10	64	59	44	35
200	4.10	7.60	8.10	7.10	73	64	46	36
250	5.50	8.50	9.10	8.10	80	77	59	38

A – SCLBRP, B-ALERT, C- ALARM, D-AASR

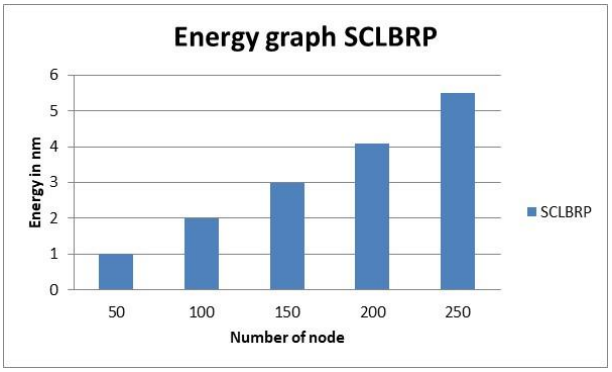

Fig 2: Energy consumption graph of **SCLBRP** method for node of 50,100,150, 200 & 250. The energy consumption of node in joules (j) or newton meter (nm).

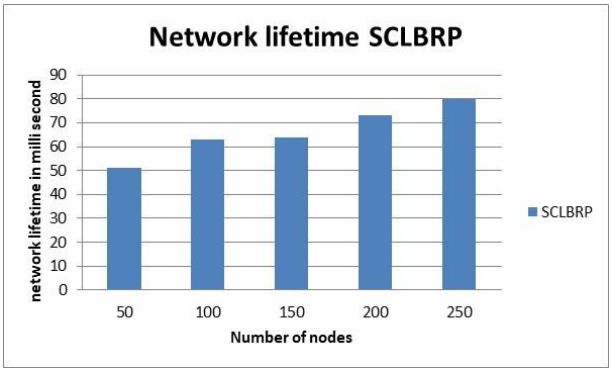

Fig 3: Network lifetime graph of SCLBRP method for node of 50,100,150, 200 & 250 and Network lifetime in mill seconds

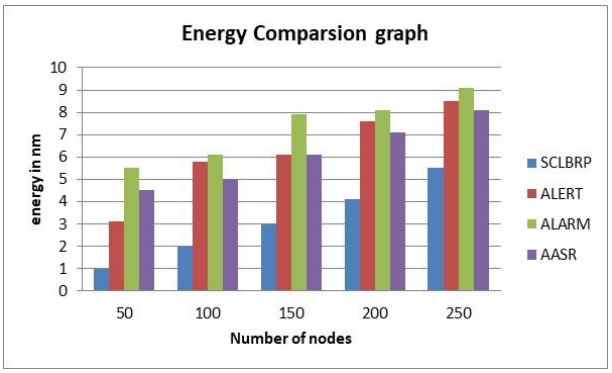

Fig 4: Energy consumption comparison graph with existing methods for node of 50,100,150, 200 & 250

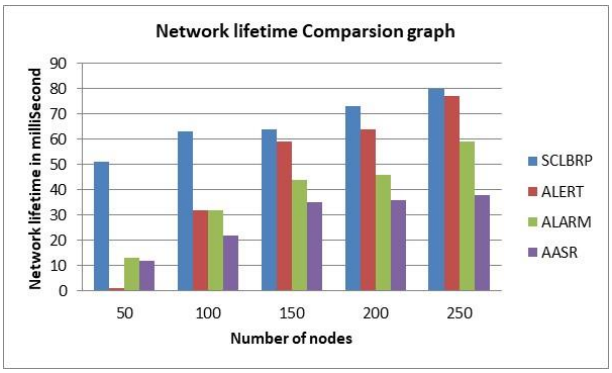

Fig 5: Network lifetime graph comparison graph with existing methods for node of 50,100,150,200 & 250.

Conclusion

The research work focused in proposing a Secure Clustered Location-Based Routing Protocol (SCLBRP) for MANET. The proposed SCLBRP protocol consists of two processes are clustering the proposed Optimal Zone Partitioning (OZP) is utilized to form the clustering and the multiple performance constraints used to compute the trust degree of each node. The highest trust degree is act as CH in the cluster among multiple mobile nodes. Optimal Trust Inference Algorithm (OTIA) is used to compute the optimal path among multiple paths. Finally, the proposed SCLBRP protocol is proved with better performance with existing protocol terms of energy and network lifetime.

References

[1] HoudaMoudni , Mohamed Er-rouidi," Secure Routing Protocols for Mobile Ad Hoc Networks", Information Technology for Organizations Development (IT4OD), 2016

[2] B. John Oommen , SudipMisra," Fault-tolerant routing in adversarial mobile ad hoc networks: an efficient route estimation scheme for non-stationary environments",Telecommunication Systems, Volume 44, Issue 1–2, pp 159–169, 2010

[3] B. John Oommen ,SudipMisra," Fault-tolerant routing in adversarial mobile ad hoc networks: an efficient route estimation scheme for non-stationary environments"Telecommunication Systems, Volume 44, Issue 1–2, pp 159–169, 2010

[4] Yuan Xue , Klaranahrstedt," Providing Fault-Tolerant Ad hoc Routing Servicein Adversarial Environments,Wireless Personal Communications, Volume 29, Issue 3–4, pp 367–388, 2004

[5] SalwaOthmen , FaouziZarai, AymenBelghith, LotfiKamoun," Anonymous and Secure On-Demand Routing Protocol for Multihop Cellular Networks", Networks, Computers and Communications (ISNCC), 2016

[6] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[7] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.

[8] H. Shen and L. Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093, 2013.

[9] W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, 2014.

[10] K. El Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345-1358, 2011

[11] Swetha, M. S., and M. Thungamani. "A novel approach to secure mysterious location based routing for manet." International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8.7 (2019): 2587-2591

[12] Mingchuan Zhang, Meiyi Yang, Qingtao Wu, RuijuanZheng, and Junlong Zhu," Smart Perception and Autonomic Optimization:A Novel Bio-inspired Hybrid Routing Protocol for MANETs"Future Generation Computer Systems ,Volume 81, Pages 505-513, 2018

[13] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad-hoc networks", Int. J. Wireless Mobile Comput., vol. 3, no. 3, pp. 145-155, Oct. 2009.

[14] Leena Jadhav, Dr. Jitendra Sheetlani, Harsh Pratap Singh "Reliable Positioning-Based Routing Using Enhance Dream Protocol in MANET" International journal of scientific & technology research volume 9, issue 01, January 2020

[15] Uma Rathore Bhatt, Neelesh Nema, Raksha Upadhyay, "Enhanced DSR: An Efficient Routing Protocol for MANET", Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014

[16] Gang, Z., Han, T., Wenwei, S., Chunfeng, L., Yantai, S., "A Hybrid DTN-DSR Routing protocol Based on Clustering", 8th International Conference on wireless communication Networking and mobile Computing (Wi COM), doi:IO.J 109IWiCOM.2012.647829J, 2012.

[17] SuparnaBiswas, Tanumoy Nag, SarmisthaNeogy," Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET" Applications and Innovations in Mobile Computing (AIMoC), 2014
[18] S.A. Abid, Mazliza Othman, Nadir Shah, Mazhar Ali , A.R. Khan," 3D-RP: A DHT-Based Routing Protocol for MANETs" The Computer Journal , Volume: 58, Issue: 2, 2015
[19] Swetha, Mrs. "Strong secure anonymous location based routing (S2ALBR) method for MANET." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.3 (2021): 4349-4356.
[20] MueenUddin, AqeelTaha, RaedAlsaqour , TanzilaSaba," Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function", IEEE Access ,Volume: 5,2017
[21] Ali Mohamed E. Ejmaa , ShamalaSubramaniam, Zuriati Ahmad Zukarnain, ZurinaMohdHanapi," Neighbor-based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network" IEEE Access , Volume: 4,2016
[22] Darren Hurley-Smith, Jodie Wetherall , Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks" IEEE Transactions on Mobile Computing , Volume: 16, Issue: 10, 2017
[23] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.
[24] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[25] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.