Educational Administration: Theory and Practice
2024, 30(5), 13652 - 13659
ISSN: 2148-2403
https://kuey.net/

Research Article

Network Initialization Using Global Authentication Scheme For Mobile Ad-Hoc Networks (Gasman)

P. Vidhya Devi[1*], Dr. B. L. Shivakumar[2]

[1*]Assistant Professor, Department of Artificial Intelligence & Data Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India. Email: ponnvidhya@gmail.com
[2]Principal, Department of Artificial Intelligence & Data Science, Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India. Email: blshiva@gmail.com

Citation: P. Vidhya Devi (2024) Network Initialization Using Global Authentication Scheme For Mobile Ad-Hoc Networks (Gasman) *Educational Administration: Theory and Practice, 30(5), 13652 - 13659*
Doi: 10.53555/kuey.v30i5.5936

ARTICLE INFO

ABSTRACT

Objectives: The objectives include proposing GASMAN, a decentralized authentication scheme for MANETs, validating its effectiveness through simulations, and discussing practical limitations and potential applications.
Methods: The Gasman authentication scheme for MANETs is presented, emphasizing its decentralized approach and ability to authenticate members without central authority. Gasman's methodology and initial simulation results using NS-2 are outlined, alongside discussions on practical limitations, potential extensions, and various application scenarios.
Findings: Gasman, a proposed authentication scheme for MANETs, offers decentralized authentication, balanced workload distribution, and adaptability to network changes. Simulation experiments conducted using NS-2 highlight its effectiveness across various scenarios, with practical limitations and potential extensions also discussed.
Novelty: Gasman introduces a novel authentication scheme tailored for MANETs, ensuring decentralized authentication without central authority, minimal information transfer, workload balance, adaptability, and extensive simulation-based validation.

Keywords: Network initialization, Secure routing, Active routing, Authentication, Mobile ad hoc networks.

1. Introduction

Mobile ad-hoc networks (MANET) are a self-configuring wireless network comprising of wireless devices with mobility [6]. MANET has the attribute of minimal arrangement and fast sending, which is reasonable for emergency circumstance scenarios like catastrophic events, military contentions and emergency medical care, and so on. Because of the attributes of network and application scenarios, the topology of Manet is variable and eccentric; carry incredible difficulties to security [10]. In Manets, conventional security measures prove ineffective. Various attack methods, such as selective forwarding attacks, false routing attacks, Byzantine attacks, etc., make the security vulnerabilities of Manets increasingly evident [20].
An ad hoc network is an assortment of wireless mobile nodes dynamically framing an impermanent network without the utilization of any current network infrastructure or centralized administration [17]. Such a network might work in a standalone style, or might be associated with the Web. Key features of Manets summed up as; No proper infrastructure, dynamic topology, power and processing imperatives, intermittent connectivity, fluctuating security necessities, scarce bandwidth and high-loss, untrustworthy links [14]. The design of suitable routing protocols is a critical test because of multihop, mobility, and the scale of the network combined with device heterogeneity, bandwidth, and battery power needs. Minimal control overhead, low processing overhead, multihop routing capability, and dynamic topology maintenance are the major objectives of an ad hoc network [7]. Routing technologies, Loop prevention, centralized versus circulated approaches, optimal route, Scalability, and Effectiveness. Giving security administrations, such as authentication, confidentiality, integrity, anonymity, and availability, is a certain goal of the security solutions for Manets, to mobile users. The network layer security

intended for Manets are worried about safeguarding the network usefulness to convey parcels between mobile nodes through multihop ad hoc forwarding [8].

2. Literature Survey

2.1 Ad Hoc On-Demand Distance Vector

Bondada P et.al proposed Key management mechanisms for data security-based routing in Mobile Ad Hoc Network [1]. In this research on Mobile Ad Hoc Networks (MANETs), security challenges are addressed through the introduction of a secure and energy-efficient routing technique employing cluster key management. The asymmetric key cryptosystem involves specialized nodes, the Calculator Key (CK) and the Distribution Key (DK), responsible for generating, verifying, and distributing secret keys. Unlike existing protocols, these nodes manage Latency and trust factors, reducing the burden on other nodes and minimizing security risks. Comparative experiments demonstrate the superior performance of the proposed protocol, establishing its effectiveness in enhancing the security and energy efficiency of MANETs over current protocols.

2.2 Anonymous Location-Aided Routing (ALARM)

El Defrawy K et.al proposed ALARM: Anonymous location-aided routing in suspect Mobile Ad Hoc Network [2]. In the realm of Mobile Ad-Hoc Networks (MANETs), preserving node anonymity and intractability becomes imperative in hostile environments. Addressing this concern, researchers present ALARM, an anonymous routing system utilizing nodes' real-time locations to establish a secure Manet map. ALARM employs advanced cryptographic techniques for node authentication, data integrity, and anonymity, mitigating the risk of insider attacks. The proposed future work involves developing a mathematical model to quantify the impact on node privacy caused by the dynamic speed and mobility patterns, specifically addressing tracking-obstruction challenges within Manets. This research signifies a crucial step towards enhancing security and privacy in dynamic and potentially adversarial Manet scenarios.

2.3 Active-Routing Authentication (AAS)

Jinbin Tu. et.al proposed an active-routing authentication scheme in Manet [3]. Mobile Ad-Hoc Networks (MANETs), known for their infrastructure-independent and decentralized nature, offer quick and adaptable networking. However, their open channels and dynamic topologies pose security risks. AAS integrates firewall strategies, expiration times, authentication node lists, and neighbor node lists to resist various attacks. Without relying on authentication algorithms, AAS significantly improves packet delivery rates by 33.9% in networks with malicious nodes. It enhances connectivity rates to 1.6 times the Cap-OLSR rate under attacks, providing valuable insights for real-world expiration time settings. Future work will explore characteristics of reactive and hybrid routing protocols for improved security scheme compatibility and address other attack modes [11].

2.4 Group Diffie Hellman (GDH) algorithm

Chhabra A et.al proposed Secure routing in multicast routing protocol for MANET's [4]. A Mobile Ad hoc Network (MANET) operates without a fixed infrastructure, enabling dynamic wireless connections among nodes that also function as routers. However, this openness poses security challenges, particularly in countering routing attacks by rogue nodes. Existing cryptographic solutions, while effective, often strain Manet's limited resources. Multicasting, transmitting messages from one node to multiple nodes, enhances key applications like tele-conferencing. The research focuses on securing Multicast routing protocols using the Group Diffie Hellman (GDH) algorithm. GDH efficiently generates keys for nodes within a group, ensuring secure communication in Manets despite mobility, random link errors, and resource constraints.

2.5 Secure Intrusion Detection System Routing Protocol

Prasad R et.al proposed MANET routing protocol for a safe intrusion detection system [5]. Recent advances in Mobile Ad-hoc Networks (MANETs) highlight their effectiveness in mobile processing, enabling seamless network connectivity. However, Manets face challenges, particularly in data transmission precision and security. Distortions in the data-link layer can jeopardize consistency, demanding corrective measures. Link-layer protocols often overlook these issues, emphasizing the need for a robust intrusion detection system. The Secure Energy Routing (SER) protocol offers a solution by integrating a Secure Intrusion Detection System (S-IDS) to bolster network security. Simulation results reveal improved packet delivery ratios and reduced end-to-end delays, affirming the protocol's efficacy in addressing security concerns within MANETs, even in the presence of attacks.

3. Proposed Methodology

In Mobile Ad-Hoc Networks (MANETs), the term network initialization encompasses the sequence of actions through which individual nodes seamlessly integrate into the network, forge communication links, and tailor their configurations to actively partake in the network's collaborative functioning. Notably distinct from conventional networks equipped with a static infrastructure, Manets stand out due to the absence of a central governing authority and the ever-changing topological landscape. In this context, nodes within Manets are

tasked with the autonomous orchestration of their organization and configuration, essential for fostering effective and adaptive communication.
The pivotal steps constituting the network initialization process in Manets include:
The GASMAN (Global Authentication Scheme for Mobile Ad-Hoc Networks) methodology introduces a comprehensive approach to secure the initialization of Mobile Ad-Hoc Networks (MANETs). This protocol is designed to ensure that all nodes within the ad-hoc network establish secure connections and trust relationships with one another.
Proposing a holistic approach, Network Initialization Using Global Authentication Scheme for Mobile Ad-Hoc Networks (GASMAN) offers a comprehensive solution for authentication in MANETs. The use of the term "GLOBAL" implies a system that extends across the entire network, providing authentication mechanisms that apply universally to all nodes.
The specific purpose of using GRP in the context of Gasman network initialization may include:

1. **Establishing Initial Communication Paths:** GRP may play a role in helping nodes discover each other during the network initialization phase. By using hop-by-hop routing, nodes can build initial communication paths to reach their destinations.
2. **Supporting Location-Based Information:** Since GRP involves geographical routing, it is likely that the protocol utilizes location information of nodes. This location-based information may be useful in Gasman's overall network initialization process, potentially aiding in the authentication and trust establishment phases.
3. **Assisting in Flooding for Node Position Updates:** The use of flooding to identify the positions of various nodes, as mentioned in the GRP description, may be a mechanism to keep track of node movements. This information could be relevant during the Gasman network initialization, especially in scenarios where nodes need to update their positions and share this information with others.

Gasman proposes a novel network initialization method for Mobile Ad-Hoc Networks. Leveraging dynamic gas-based algorithms, it aims to enhance efficiency, adaptability, and seamless communication in evolving network environments [22]. There are many routing protocols in the ad hoc environment and some of them contain secure extension to carry out security solution [16].

3.1 Secure Mobile Ad Hoc Network Design and Attacks

The Manet was established for a campus consists of 30 mobile nodes; the nodes are distributed randomly within an 800x800 m area, and each node moves uniformly at a speed of 10 m/s following a random mobility waypoint profile. [12]. A rectangular area that a site will move within during a simulation is defined by random mobility. For mobile sites, deterministic pathways are specified via trajectories and orbits.

3.2 Geographic Routing Protocol (GRP)

Geographical Routing Protocol (GRP) is a proactive routing protocol with hop by hop routing. The GRP protocol, which is source initialized in MANET routing, allows source nodes in mobile ad hoc networks to establish all routing paths. The source node in this protocol gathers all the data regarding the path to the designated location. A packet that named Destination Query (DQ) is used continuously to forward to each neighbor node until the destination is reached. The destination node transmits a network information gathering (NIG) packet to its peers upon reaching its destination. A node broadcasts Hello messages on a regular basis to keep track of its adjacent nodes. If a node does not receive a Hello message from a nearby node for duration longer than the designated "Neighbor Expiry Time," it presumes that the neighbor has lost contact. It is assumed that every node can determine its own position using a Global Positioning System (GPS). Flooding is a technique used to identify the positions of various nodes. A node transmits a flooding message with its new position whenever it moves more than a predetermined distance.

3.3 GASMAN Network Initialization

The Gasman network initialization process is an essential component of the overall Gasman methodology. It is responsible for ensuring that all nodes in the ad-hoc network are securely connected and have established trust relationships with each other.
There are three stages to the suggested Gasman network startup procedure:
1. Node Registration Phase: In this phase, each node in the network generates a public and private key pair using asymmetric encryption techniques. This process can be expressed as eq. (1),

$$KeyPairRSA = GenerateRSAKeyPair() \quad (1)$$

Subsequently, the public key is disseminated to all other nodes through broadcasting by eq. (2):

$$Broadcast(KeyPairRSA.PublicKey) \quad (2)$$

Simultaneously, each node generates a secret key using the AES encryption algorithm, denoted as eq. (3),

$$KeyAES = GenerateAESKey()KeyAES = GenerateAESKey() \quad (3)$$

2. Authentication Phase: Moving to the Authentication Phase, the public keys of two communicating nodes are exchanged, symbolized by eq. (4),

$$Node1 \leftrightarrow Node2: Exchange(KeyPairRSA1.PublicKey, KeyPairRSA2.PublicKey) \quad (4)$$

Following this, each node validates the authenticity of the counterpart's public key by cross-referencing it with its list of trusted nodes eq. (5):

$$Node1: VerifyAuthenticity\begin{pmatrix} ReceivedPublicKey2, \\ ListTrustedNodes1 \end{pmatrix} \quad (5)$$

Upon successful verification, the nodes exchange their secret keys using asymmetric encryption techniques, encapsulated in the eq. (6):

$$Node1 \leftrightarrow Node2: Exchange(EncryptRSA(KeyAES1, PublicKey2), EncryptRSA(KeyAES2, PublicKey1)) \quad (6)$$

3. Network Initialization Phase: The final Network Initialization Phase sees each node creating a list of trusted nodes based on verified public keys in eq. (7):

$$(Node: CreateListTrustedNodes\ (PublicKeysAllNodes) \\ Nodei: CreateListTrustedNodesi\ (PublicKeysAllNodes)). \quad (7)$$

This list is instrumental in ensuring that communication exclusively occurs among trusted nodes. Furthermore, every node broadcasts its compiled list of trustworthy peers to the entire network, expressed as eq. (8),

$$Node \leftrightarrow Node: Broadcast(ListTrustedNodes) \\ Nodei \leftrightarrow Nodej: Broadcast(ListTrustedNodesi) \quad (8)$$

The Gasman network initialization algorithm can be summarized as follows:

Step 1: Node Registration Phase
a. Each node generates a unique public and private key pair using the RSA encryption algorithm.
b. The public key is broadcasted to all other nodes in the network.
c. Each node generates a secret key using the AES encryption algorithm.
Step 2: Authentication Phase
a. The public keys of two nodes are exchanged when research wish to communicate.
b. Each node verifies the authenticity of the other node's public key by checking whether it is in its list of trusted nodes.
c. Once the authenticity of the public key is confirmed, the nodes exchange their secret keys using asymmetric encryption techniques.
Step 3: Network Initialization Phase
a. Each node creates a list of trusted nodes by verifying their public keys.
b. The list of trusted nodes is used to ensure that only trusted nodes can communicate with each other.
c. Every node in the network publishes its list of trustworthy peers to every other node.

In this research, the proposed GASMAN methodology uses a combination of asymmetric and symmetric encryption techniques to provide secure communication between nodes in a Manet. The algorithm ensures that only trusted nodes are allowed to communicate with each other, and all data is encrypted using a shared secret key.

The division of the network initialization process into well-defined phases provides a systematic and efficient approach to setting up the network, contributing to organized and streamlined operations. The approach is applicable to Mobile Ad-Hoc Networks (MANETs), showcasing adaptability to dynamic and decentralized network environments, while its structured nature makes it scalable for networks of varying sizes and configurations.

4. Experimental Results

4.1 Availability

Availability represents the system's operational time proportion, accounting for both mean times between failures (MTBF) and mean time to repair (MTTR).

$$Availability = \frac{MTBF}{MTBF + MTTR} \quad (9)$$

Table 1.Comparison table of Availability

Number of Nodes	GDH	ALARM	Proposed GASMAN
100	78.12	84.37	98.67
200	76.69	82.82	96.26
300	74.62	80.54	95.21
400	72.55	78.63	92.58
500	69.94	74.72	89.87

The Comparison Table 1 of Availability demonstrates the different values of existing GDH, ALARM and Proposed GASMAN. When contrasting the current algorithm with the proposed GASMAN, the latter yields superior outcomes. The current values of the algorithm range from 69.94 to 78.12 and 74.72 to 84.37 and Proposed GASMAN values starts from 89.87 to 98.67. The proposed method provides the great results.

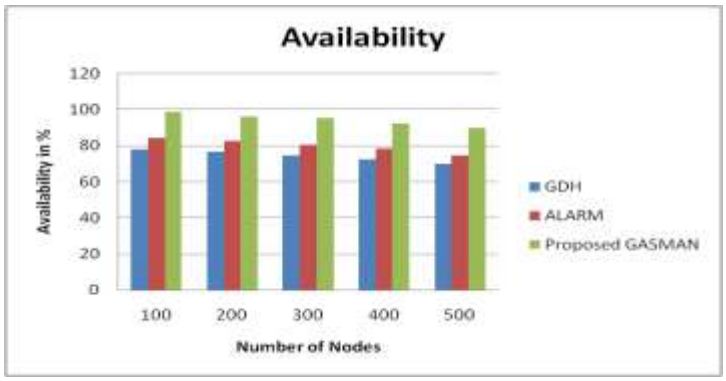

Figure 1.Comparison chart of Availability

The Figure 1 Shows the comparison chart of Availability demonstrates the existing GDH, ALARM and Proposed GASMAN. X axis denote the Number of Nodes and y axis denotes the availability ratio in %. The Proposed GASMAN values are better than the existing algorithm. The existing algorithm values start from 69.94 to 78.12 and 74.72 to 84.37 and Proposed GASMAN values starts from 89.87 to 98.67. The proposed method provides the great results.

4.2 Latency

Latency measures the time lapse from initiating a process to receiving its response, indicating system responsiveness.

$$Latency = Time_{response} - Time_{initiation} \quad (10)$$

Table 2. Comparison table of Latency

Number of Nodes	GDH	ALARM	Proposed GASMAN
100	2.12	1.37	0.82
200	2.2	1.82	0.88
300	2.32	1.54	0.99
400	2.35	1.63	1.2
500	2.04	1.72	1.41

Table 2 compares Latency values between existing GDH and ALARM algorithms and the proposed GASMAN. GASMAN outperforms the existing algorithm, with values ranging from 0.82 to 1.41 compared to the current algorithm's range of 1.37 to 1.82 and 2.04 to 2.35. The suggested approach consistently delivers superior results, showcasing its efficiency in Latency management.

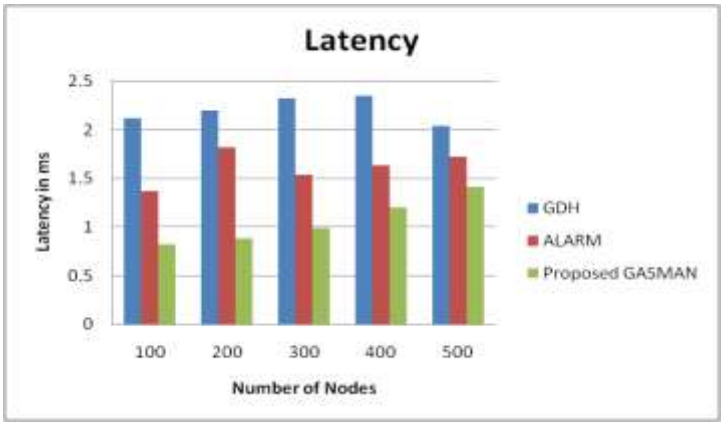

Figure 2. Comparison chart of Latency

Figure 2 illustrates a Latency comparison chart among existing GDH and ALARM algorithms and the proposed GASMAN. Nodes are plotted on the x-axis, and latency ratios in ms on the y-axis. GASMAN surpasses current algorithms, with values ranging from 0.82 to 1.41, outperforming the existing algorithm values of 1.37 to 1.82

and 2.04 to 2.35. The proposed GASMAN demonstrates superior performance, yielding exceptional outcomes in Latency.

4.3 Efficiency

Efficiency quantifies the utilization of resources in achieving the experiment's objectives, reflecting effectiveness in resource allocation.

$$Efficiency\ (E) = \frac{Output\ Achieved}{Resources\ Consumed} \quad (11)$$

Table 3. Comparison table of Efficiency

Number of Nodes	GDH	ALARM	Proposed GASMAN
100	66.94	74.91	88.01
200	69.66	71.77	91.87
300	74.12	67.93	93.48
400	79.09	68.05	94.23
500	86.38	65.39	96.52

In the Efficiency Comparison Table 3, existing GDH and ALARM algorithms are compared with the proposed GASMAN. The results indicate GASMAN outperforms the current algorithms, exhibiting values ranging from 88.01 to 96.52. In contrast, existing algorithms show values between 66.94 to 86.38 and 65.39 to 74.91. The proposed GASMAN method consistently delivers superior results, showcasing its effectiveness in enhancing Efficiency measures.

Figure 3. Comparison chart of Efficiency

Figure 3 illustrates an Efficiency comparison among existing GDH, ALARM, and the proposed GASMAN. The x-axis represents the Number of Nodes, while the y-axis indicates the Efficiency ratio in %. GASMAN outperforms existing algorithms, showing values ranging from 88.01 to 96.52, surpassing 66.94 to 86.38 and 65.39 to 74.91. The proposed method demonstrates significant improvements in achieving enhanced Efficiency outcomes.

4.4 Scalability

Scalability refers to a system's capability to effectively manage data volumes without compromising performance or functionality.

$$Scalability\ = \frac{Data\ Volume}{System\ Capacity} (12)$$

Table 4. Comparison table of Scalability

Number of Nodes	GDH	ALARM	Proposed GASMAN
100	78	85	97
200	74	87	96
300	71	83	94
400	69	81	92
500	65	78	90

Table 4, comparing Scalability Values for existing GDH and ALARM with Proposed GASMAN, highlights the latter's superior performance. Current algorithm values range from 0.80 to 0.88 and 0.63 to 0.73, while Proposed GASMAN achieves higher values, ranging from 0.92 to 0.98. The proposed method consistently delivers superior results, showcasing its effectiveness in scalability over existing algorithms.

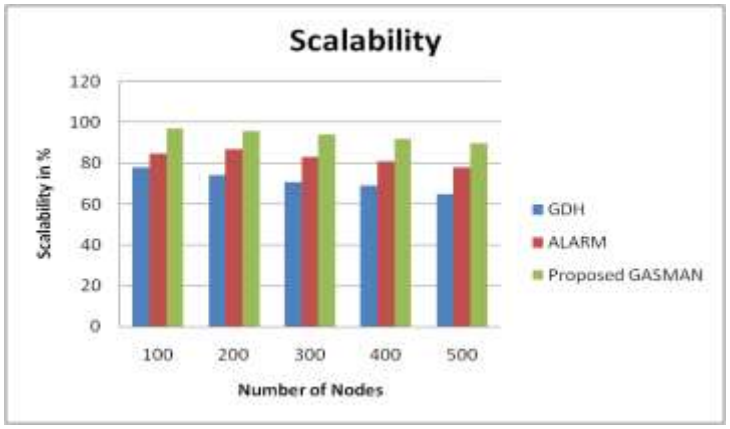

Figure 4. Comparison chart of Scalability

Figure 4 depicts a Scalability comparison chart among existing GDH and ALARM algorithms and the proposed GASMAN. The x-axis represents the Number of Nodes, and the y-axis shows the Scalability ratio in %. GASMAN outperforms existing algorithms, with values ranging from 0.92 to 0.98, compared to the current algorithmic range of 0.80 to 0.88. The suggested approach demonstrates superior outcomes, with values ranging from 0.63 to 0.73 for the existing algorithms.

5. Conclusion

In this paper proposed the GASMAN authentication scheme provides a strong and adaptable method for secure communication in mobile ad-hoc networks without the need for centralized authority. The proposed scheme offers a balanced workload for legitimate members and can react to network topology changes. Further studies on practical limitations, different applications, and possible extensions of Gasman are recommended. The initial simulation using NS-2 network simulator is promising and further results will be included in a future version of the work.

6. References

1. Bondada P, Samanta D, Kaur M, Lee HN. Data security-based routing in MANETs using key management mechanism. *Applied Sciences*. 2022 Jan 20;12(3):1041.
2. El Defrawy K, Tsudik G. ALARM: Anonymous location-aided routing in suspicious MANETs. *IEEE Transactions on Mobile Computing*. 2010 Dec 30;10(9):1345-58.
3. Tu J, Tian D, Wang Y. An active-routing authentication scheme in MANET. *IEEE Access*. 2021 Jan 27; 9:34276-86.
4. Chhabra A, Arora G. Secure routing in multicast routing protocol for MANET's. *International Journal of Innovations in Engineering and Technology*. 2013;2:1-8.
5. Prasad R. Secure intrusion detection system routing protocol for mobile ad-hoc network. *Global Transitions Proceedings*. 2022 Nov 1; 3(2):399-411.
6. Singh V., and M. Jain, "Analysis of trust dynamics in cyclic mobile: Ad hoc networks," *International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*, Greater Noida, India, 2015, pp. 400-406, doi: 10.1109/ABLAZE.2015.7155029.
7. Caballero-Gil P., C. Caballero-Gil, J. Molina-Gil and C. Hernandez-Goya, "Self-organized authentication architecture for Mobile Ad-hoc Networks," *2008 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops*, Berlin, Germany, 2008, pp. 217-224, doi: 10.1109/WIOPT.2008.4586067.
8. Karimou D. and J. F. Myoupo. An energy-saving algorithm for the initialization of single hop mobile ad hoc networks, *Systems Communications (ICW'05, ICHSN'05, ICMCS'05, SENET'05),* Montreal, Quebec, Canada, 2005, pp. 153-158, doi: 10.1109/ICW.2005.26.
9. Chih-Shun Hsu and Jang-Ping Sheu. Initialization protocols for IEEE 802.11-based ad hoc networks, *Ninth International Conference on Parallel and Distributed Systems, 2002.* Proceedings., Taiwan, 2002, pp. 273-278, doi: 10.1109/ICPADS.2002.1183411.
10. Raskar S. and K. Iyer. Performance Comparison on Path Establishment and Recovery algorithms in Wireless Ad-Hoc Networks. *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*, Sangamner, India, 2018, pp. 372-377, doi: 10.1109/ICACCT.2018.8529618.
11. S. Manjula and Suresh. Reliable and scalable technique with efficiency in hybrid Network. *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 899-904, doi: 10.1109/I-SMAC.2017.8058310.

12. Chen L. -q., and R. -l. Hu. An Efficient Group Key Agreement Scheme for MANETs Based on Merkle Identity Tree. *Second World Congress on Software Engineering*, Hubei, China, 2010, pp. 151-154, doi: 10.1109/WCSE.2010.16.
13. Al-hemyari A., K. Jumari, M. Ismail and S. Saeed. *A comparative survey of multicast routing protocol in MANETs*. International Conference on Computer & Information Science (ICCIS), Kuala Lumpur, Malaysia, 2012, pp. 830-835, doi: 10.1109/ICCISci.2012.6297141.
14. Abassi R. and S. G. E. Fatmi. Dealing with delegation in a trust-based MANET, *ICT* 2013, Casablanca, Morocco, 2013, pp. 1-5, doi: 10.1109/ICTEL.2013.6632099.
15. Dahshan H. and J. Irvine. A Threshold Key Management Scheme for Mobile Ad Hoc Networks Using Elliptic Curve Dlog-Based Cryptosystem. *8th Annual Communication Networks and Services Research Conference,* Montreal, QC, Canada, 2010, pp. 130-137, doi: 10.1109/CNSR.2010.48.
16. Othmen S., A. Belghith, F. Zarai, M. S. Obaidat and L. Kamoun. Power and Delay-aware Multi-Path Routing Protocol for Ad Hoc Networks. *International Conference on Computer, Information and Telecommunication Systems (CITS),* Jeju, Korea (South), 2014, pp. 1-6, doi: 10.1109/CITS.2014.6878956.
17. Caballero-Gil P., C. Caballero-Gil, J. Molina-Gil and C. Hernandez-Goya. Self-organized authentication architecture for Mobile Ad-hoc Networks. *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops*, Berlin, Germany, 2008, pp. 217-224, doi: 10.1109/WIOPT.2008.4586067.
18. Taghiloo M, Dehghan M, Taghiloo J, Fazio M. New approach for address auto-configuration in MANET based on virtual address space mapping (VASM). In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications* 2008 Apr 7 (pp. 1-6). IEEE.
19. Singh A, Maheshwari M, Kumar N. Security and trust management in MANET. *In Information Technology and Mobile Communication: International Conference, AIM* 2011, Nagpur, Maharashtra, India, April 21-22, 2011. Proceedings 2011 (pp. 384-387). Springer Berlin Heidelberg.
20. Venkatasubramanian S, Suhasini A, Vennila C. Efficient multipath zone-based routing in MANET using (TID-ZMGR) ticked-ID based zone manager. *International Journal of Computer Networks and Applications (IJCNA)*. 2021;8(4):435-43.
21. Al-Shidi Q., A. Alburaiki, H. Shaker and B. Kumar. Q-Analyze Tool to Detect Malicious and Black Hole Nodes in NS2 Simulation for AODV. *International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, India, 2018, pp. 140-146, doi: 10.1109/SYSMART.2018.8746938.
22. Caballero-Gil P, Caballero-Gil C, Molina-Gil J, Hernández-Goya C. Self-organized authentication architecture for Mobile Ad-hoc Networks. *In 2008 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops* 2008 Apr 1 (pp. 217-224). IEEE.
23. Apetroaie-Cristea M. A modular and open software and hardware architecture for internet of things sensor networks. *Doctoral dissertation, University of Southampton*.
24. Elkrunz H. The Role of Implementing Mobile Business Intelligence (MBI) in Decision Making Process: *An Empirical Study at Jawwal Company*. Available at SSRN 2450958. 2013.
25. Edmunds PJ, McIlroy SE, Adjeroud M, Ang P, Bergman JL, Carpenter RC, Coffroth MA, Fujimura AG, Hench JL, Holbrook SJ, Leichter JJ. Critical information gaps impeding understanding of the role of larval connectivity among coral reef islands in an era of global change. *Frontiers in Marine Science*. 2018 Aug 27; 5:290.