International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Effective Key Management Protocol on AODV for Group Security

Bhawna Sharma [1], Rohit Vaid [2]

Submitted: 10/05/2023 **Revised**: 17/07/2023 **Accepted**: 08/08/2023

Abstract: Mobile Ad Hoc Networks, or MANETs, are decentralised networks made up of mobile devices that can connect with one another without the use of a centralised infrastructure. Because MANETs are dynamic and self-organizing, securing data transfer presents specific difficulties, particularly with regard to routing algorithms. By providing authentication and confidentiality for communication among the participating nodes, the Key Management Protocol for MANET Routing Group Security is a protocol created to secure the routing operations within a MANET. In this study, group communication security is provided using a combination of the RSA and DH (Diffie-Hellman) algorithms. Utilizing metrics like routing overhead, throughput, and security level, the performance of this ensemble key management system is evaluated for the AODV. After using this technique, we discovered that our suggested ensemble method secures group communication as compared to Diffie-Hellman, improves throughput by altering the quantity of messages sent, and decreases routing overhead in various groups. Group security over Diffie-Hellman was boosted by 30% by combining RSA and DH.

Keywords*: MANET, Routing protocols, key management, AODV, group key management, RSA and DH.*

1. Introduction

A cryptographic tool called the Key Management Protocol (KMP) for Mobile Ad hoc Network (MANET) Routing Group Security was created to protect the routing protocols used in MANETs. Mobile nodes in MANETs are self-configuring, infrastructure-free networks that can connect with one another without the aid of a centralised infrastructure[1]. Routing protocols are essential for creating and maintaining communication channels between nodes in MANETs. Yet, MANETs' dynamic nature and the lack of a reliable central authority present serious security difficulties. Keeping routing information transferred between nodes discreet, legitimate, and authentic is one such difficulty. The KMP for MANET Routing Group Security provides a framework for secure key management within the routing group in order to address these difficulties[2]. A group of cooperating nodes that take part in the routing protocol is referred to as the routing group. To enable secure communication, the key management procedure entails the creation, distribution, and upkeep of cryptographic keys among the group members.

The following steps are often included in the protocol:

• Key Establishment: Establishing a common secret key between the group members is the first stage. This can be accomplished using a variety of methods, including pre-distribution of keys or symmetric or asymmetric key exchange.

• Key Distribution: Once the shared key has been created, it must be safely delivered to each group member. The key can be encrypted using the recipients' public keys when employing secure multicast or broadcast techniques.

• Key Refreshment: Nodes may eventually join or leave the routing group since MANETs are dynamic. Key refreshment techniques make ensuring that keys of departing nodes are updated or revoked and that new nodes joining the group receive the appropriate keys.

• Key Revocation: To keep the group's overall security, a node's key must be revoked when it is compromised or quits the group. To revoke the compromised or out-of-date keys, key revocation techniques are used.The routing protocols must be protected from attacks including eavesdropping, message tampering, spoofing, and insider threats by the KMP for MANET Routing Group Security. The protocol guarantees confidence and confidentiality in the routing information exchanged between nodes and ensures the overall security and stability of the MANET by creating and preserving secure keys within the routing group[3].

The Distributed Security Strategy for MANET (DSSM) and the Secure and Efficient Group Key Management System are two KMPs that were created specifically for MANETs (SEGK). These protocols offer different key creation, distribution, and management strategies, but they all work to make MANET routing methods more secure.

1.1 Advantages of Key Management Protocol's

There are various benefits that the Key Management Protocol for MANET Routing Group Security provides that improve the overall security and sturdiness of Mobile Ad Hoc Networks (MANETs). These are a few significant benefits:

[1,2] *Department of Computer Science and Engineering, MMEC, MM (Deemed to be University), Mullana, Ambala, India*
[1] *ORCID ID : 0009-0004-3826-4930*

** Corresponding Author Email: bsbhawna90@gmail.com*

Authentication: The protocol offers a method for MANET participant nodes to authenticate one another. It guards against unwanted access and guarantees that only authentic nodes can join the network by confirming the identification of nodes. The MANET's overall security is improved by this authentication method.

Confidentiality:The protocol creates and maintains cryptographic keys for nodes to use in secure communication. It guarantees confidentiality by encrypting the data sent between nodes, preventing unauthorised nodes or adversaries from listening in on confidential information. This safeguards the confidentiality of data transferred within the MANET.

Data Integrity: Data integrity is guaranteed by the protocol through the use of cryptographic keys. It gives nodes the ability to check the accuracy of data they have received, guarding against data manipulation or change during transmission. This guarantees the integrity and reliability of the information exchanged within the MANET[4].

Key Distribution Efficiency: The protocol uses effective methods for key distribution and establishment among nodes. It minimises key management overhead, which lowers the demand on computing and communication resources. Efficiency like this is essential in dynamic MANETs, where nodes periodically join and depart the network.

Scalability: The protocol is made to grow in size along with the MANET's size and the number of participating nodes. It is capable of handling massive MANET installations without jeopardising security or adding a lot of overhead. To accommodate various application scenarios and network sizes, this scalability is crucial.

Group Management: Within the MANET, the protocol permits the establishment and administration of routing groups. Establishing group-specific security policies enables fine-grained control over the security measures implemented for various subsets of nodes. The flexibility and adaptability of security setups are improved by this group management feature.

Resilience to Compromised or Departing Nodes: When a node is compromised or leaves the network, the protocol manages key revocation. It stops compromised nodes from gaining access to the network or jeopardising the security of other nodes by cancelling compromised or out-of-date keys. This increases the MANET's overall resistance to security threats[5].

The Key Management Protocol for MANET Routing Group Security considerably improves the security posture of MANETs by offering authentication, confidentiality, integrity, effective key management, scalability, and group management capabilities. In dynamic and self-organizing networks, it enables trusted and secure communication between nodes, reducing the dangers of illegal access, data manipulation, and eavesdropping.

1.2 Key Management Protocol Types for MANET

Key Management Protocols for MANET Routing Group Security come in a variety of forms. Here are a few often employed types:

Centralized Key Management Protocols: The cryptographic keys for the MANET's participating nodes are created, distributed, and managed by a central authority or key management server according to these protocols. The distribution, establishment, and authentication of keys are all handled by the central authority. The Key Management Scheme (KMS) and Key Distribution Center (KDC)-based protocols are examples of centralised key management protocols.

Decentralized Key Management Protocols: These protocols divide up the key management duties among the MANET's participating nodes. There is no need for a centralised authority because each node participates to the crucial establishment and dissemination operations. Group key management strategies, which enable subsets of nodes to cooperatively handle the keys for their respective routing groups, are frequently used in decentralised protocols[6]. The Tree-Based Group Key Management Protocol (TGKMP) and the Distributed Group Key Management Protocol are two examples of decentralised key management systems (DGKMP).

Hierarchical Key Management Protocols: The MANET nodes are arranged into a hierarchical structure using hierarchical protocols, where nodes are organised into clusters or tiers. A selected cluster head is in charge of key management for each individual cluster. To establish and distribute keys, the cluster leaders converse with one another, ensuring safe routing group communications. The overhead involved with group key management is intended to be minimised using hierarchical key management systems. Hierarchical key management protocols include the Hybrid Key Management Protocol (HKMP) and the Multilevel Key Management Protocol (MKMP)[7].

Self-Organizing Key Management Protocols: Since nodes often join and depart MANETs, these protocols are made to adapt to their dynamic character. With the use of self-organizing key management protocols, nodes can create and maintain keys on their own without the need for a centralised authority or set structure. To maintain secure group communications, these protocols frequently use techniques like self-certification, distributed key establishment, and dynamic key update algorithms[8]. The Self-Organizing Key Distribution Protocol (SOKDP) and the Self-Organized Hierarchical Key Management Protocol are two examples of self-organizing key management

protocols (SOHKMP).

The key management protocol types for MANET routing group security are only a few examples. In a particular MANET deployment scenario, variables including network characteristics, security needs, scalability, and overhead concerns affect the protocol choice.

2. Related Work

Author	Analysis
Shu et al [11]	Use randomised dispersive routes for wireless sensor networks in MANET to collect data securely. It created methods for creating arbitrary multipath routes.
Burmester et al. [10]	MANET created a QoS self-optimization to deliver a satisfied QoS. (Service Quality). Using the idea of signal space diversity, a single-hop transmitting system with a direct link between the source and the destination is evaluated.
Mohindra et al[8]	For the multi-party Diffie Hellman group key exchange-based password-authenticated group protocol, commonly known as group key agreement, a methodical key distribution methodology was developed. The protocol's main goal is to create and distribute a secret session key, symbolised by "K," among a group of nodes or customers who need a secure connection.
Manjula et al., [14]	The group uses a cutting-edge clustering methodology, utilizing scalable key management techniques to create clusters based on node affinity relationships. They provide two types of cluster head-generated keys for safe connections, accommodating dynamic topology changes and battery power restrictions.
Wan et al., [15]	A distributed certification facility was provided in addition to a predictable security paradigm. A network forms clusters, each with a unique head node. These nodes operated as administrative hubs and shared a network key with other cluster members. A comparable key is also used for certification. The cluster is constructed and configured by the cluster head (CH), the sole unique node in each cluster.

3. Key management

Key management in ad hoc networks is challenging since it's challenging to ensure that a resource, The secrecy and integrity of a communication are reduced by cryptography to the confidentiality and integrity of a key (fig 2). The nodes in symmetric key cryptography must concur on a secret key [13]. Methods for creating a secure key and rekeying it while minimising storage and transmission overhead present issues [16][19].

There are three types of key distribution systems:

1) pre-distribution schemes
2) Systems involving a trusted third party, and
3) Techniques based on public key cryptography.

A. Secure Group communication

Secure communication is possible in two situations: 1) communication between all nodes, and 2) communication between specific nodes.

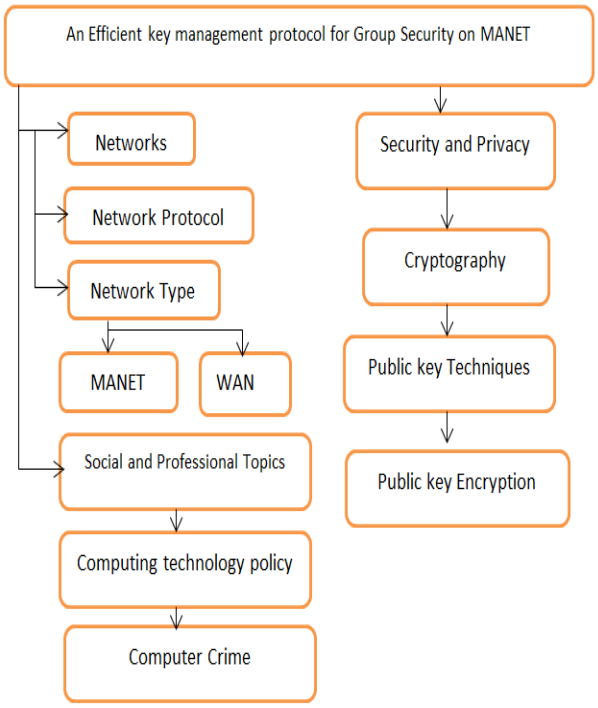

Fig.2 An Efficient key management protocol for Group Security on MANET Routing Protocol

1. Communication across all nodes: During this exchange, group members use a symmetric key encryption technique to encrypt data before sending it to other nodes. Using this algorithm, cypher text is produced as the output, with data and the group key serving as the input. As seen in Figure 3, this cypher text was decoded by all nodes using the group key [18].

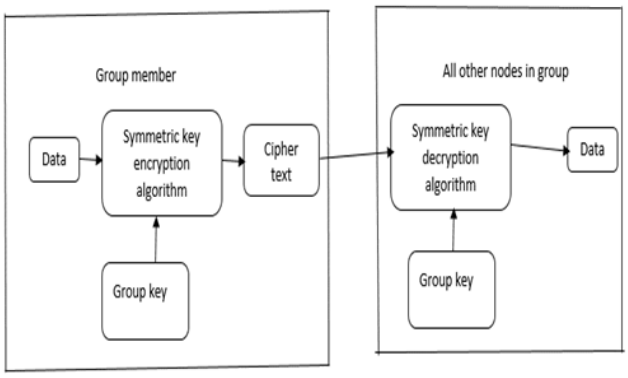

Fig 3: Communication between all nodes

2. Communication between chosen nodes: When a node wants to communicate with another node in the group, it uses the symmetric key encryption technique to encrypt the data with a shared key. Crypher text is the output of this method. shared key is encrypted with the recipient's public key to increase security. According to Fig. 4, the receiver uses its own private key [20] to decode the shared key.

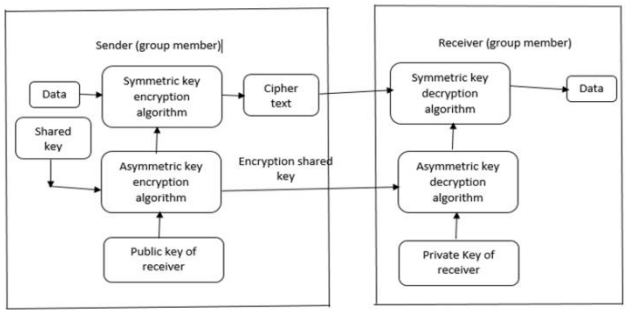

Fig 4: Communication between selected nodes

AODV with key management

Because it was designed primarily for routing on mobile ad hoc networks, the Ad hoc On-Demand Distance Vector (AODV) protocol does not by default provide security capabilities for group communication or key management (MANETs). However, AODV could be made better by incorporating more security measures to offer keyed secure group communication. To enable secure group communication with AODV, secure key management and key distribution mechanisms would need to be used. The following is a general overview of how you may approach achieving it:

3. Secure Group Formation: Before setting up secure group communication, the group must be safely formed. This often involves deciding on a standard group key and appointing a group controller or leader during the group setup stage.

4. Key Distribution: The group leader can distribute the group key to the group members using a secure key distribution method. This protocol ensures that the shared key is communicated with confidentiality, integrity, and validity. Methods like asymmetric encryption (like RSA) or symmetric encryption (like AES) can be used for secure key distribution.

5. Key Management: Once the group key has been distributed, the group members can use it to encrypt and decrypt their communication. Key updates, key revocation, and safe key storage are methods used in key management. These methods are essential to the continued security and dependability of group communication.

6. Secure Routing: To ensure safe communication within the group, security components must be included to the AODV routing protocol. Routing control messages may need to be protected from manipulation or impersonation attacks, route discovery and maintenance methods may need to be secured, and authentication techniques to verify the legitimacy of participating nodes may need to be implemented.

7. Group Communication: Once a secure group has been established and the keys have been distributed, the group members can communicate using the AODV protocol. They would encrypt their messages using the shared group key to ensure that only authorised members could decrypt and access the data.

Keep in mind that using keys to establish secure group communication in AODV presents additional challenges that go beyond the scope of the original AODV protocol. Therefore, a thorough understanding of network security principles and cryptographic algorithms is necessary to design and implement a trustworthy and secure system.

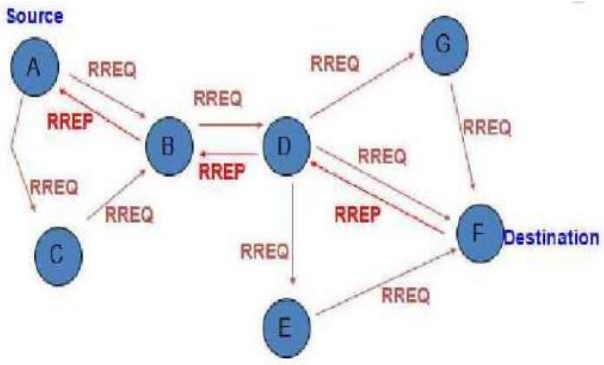

Fig. 5 RREQ and RREP in AODV [8]

Proposed Algorithm

1.Choose A and B, two huge prime numbers.

2. Determine N = A x B.

3. Choose EK as the public key (EK) so that it is not a factor of (A – 1) and not for (A – 1). (B -1).

4. Choose DK as the private key (DK) so that the equation (DK x EK) mod (A – 1) x (B – 1) = 1 is true.

5. Assume U, S, and Q are prime constants created automatically.

6. Assign the values of EK and DK from the previous step to the secret number A=EK and B=DK.

7. Now, as a public number, compute the following.

1. QA mod U = X

2. Y= QB mod U

Formula is used to calculate the session key.

1. KA = YA mod U (or KA = YA mod U) (QB mod U) A mod U or KA = (QB) A mod U or KA = (QB) A mod U or KA = QBA mod P.

2. KB = XB mod U or KB = KB = KB = KB = KB = KB = KB = KB (QA mod U)

(QA) B mod U or KB = QAB mod U. 3. B mod U or KB = (QA) B mod U or KB = QAB mod U. As a result, KA = KB = K.

To generate a new CT, we XOR session key K with PT: For encryption, CT = PT XOR K.

After that, transfer CT to the receiver for decryption, and compute PT from CT:CT XOR K = P

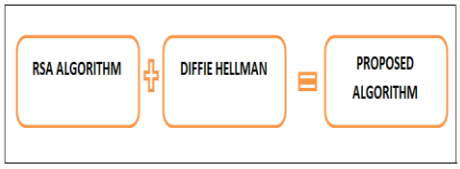

Fig 6: A Proposed Algorithm (RSA+DH)

No other MANET group has access to data that is solely approved to that group, and members of the Security Group have exclusive access to their permitted data. Security for the group is very high. On the basis of the research done on routing mechanisms and key management systems, new approaches for overcoming such difficulties must be given. It is necessary to provide a special methodology for establishing reliable pathways for securely transmitting data.

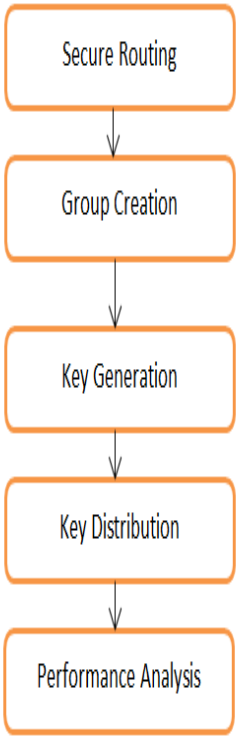

Fig 7: Proposed Framework

4. Simulation Results and Analysis on Aodv Protocol

A routing-based data security procedure in MANET can be implemented using the suggested method for group security employing key management, enabling secure data communication AODV. The proposed method (RSA+DH) is applied in the NS-2 simulator.

Routing overhead: Because MANET has a dynamic topology, it is possible for a group's member to break off. As a result, when applying (RSA+DH) to that group, the members' area keys might be modified. Overhead rekeying takes place as you go. There is a greater rekeying overhead when a member leaves the MANET's domain.

Table 1: No. of groups to the Rekeying overhead

No. of groups	RSA+DH Method	DH Method
1	8	12
2	11	14
3	13	16
4	16	19

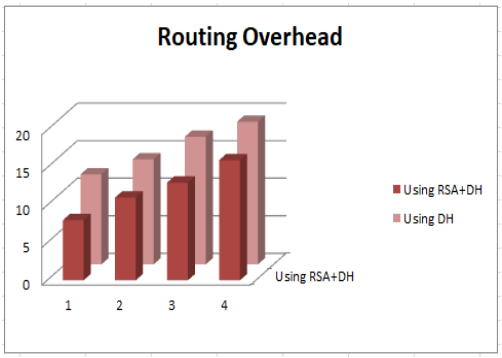

Fig 8: No. of groups to the Routing overhead

The process of routing overhead coming from secure groups created in AODV in MANET is depicted in Fig. 6 using the suggested approach. The danger of routing overhead is decreased with the suggested solution. There is less chance of routing overhead because the suggested technique (RSA+DH) transmits packet data via a data security mechanism. The performance of the suggested solution in terms of routing overhead is shown in Fig 7. The proposed methodology would reduce routing overhead while forwarding packet data from source to destination by 12–24% when compared to present methods (DH).

Throughput: In MANET communication, it is the typical rate of successfully transmitting messages from one group to another. Power is often measured in bits per second (bps), although it can also be expressed as packets per second or packets over time. Table 2 displays the throughput in percentages for successful MANET message transmission.

TABLE 2: THE RATIO OF THE NUMBER OF MESSAGES IN GROUPS TO THE THROUGHPUT

No. of messages (groups)	***A Proposed (RSA+DH)***	***DH (Method)***
10	25	10
20	34	19
30	40	25
40	45	34

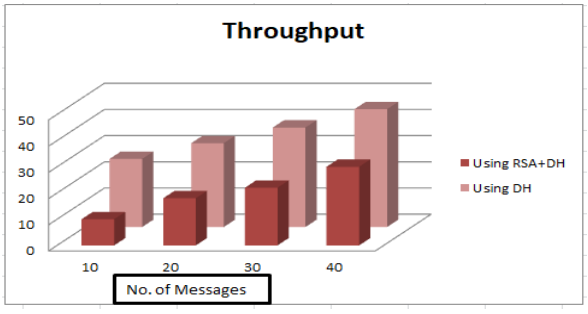

Fig 9: The Ratio of the Number of Messages in Groups to the Throughput

Fig. 9 displays the throughput for efficient message transmission in a MANET utilising the new approach (RSA+DH). The proposed method has a high data delivery rate because the group has been proven to securely use keys in MANET. This method uses data security to transmit packet data, therefore the route discovery stage is carried out first.

Here, the throughput performance of the suggested approach is shown. The proposed method would have a nearly 80% larger variance in packet or data delivery throughput from source to destination when compared to a current DH. Look at Table 3.

Table 3: Group Security level in MANET

Group Security level (%)		
Method used	(RSA+DH)	DH Method
	80	50

5. Conclusion

Key management using RSA+DH for group security offers the best performance for mobile ad-hoc networks. As a result, clustering nodes in AODV increases network traffic and productivity with little additional expense. Group-based networks can thus achieve good scalability. The routing overhead, throughput, and security level were among the various factors used to examine the performance. After using the ensemble (RSA+DH) algorithm, we discovered that our suggested method provides security that is roughly 80% secure as compared to the conventional DH method while reducing the routing overhead and improving throughput, that is, the rate of successfully received packets. Future upgrades to this technology will include choices for real-time data processing and transmission.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Jain S, Agrawal K. The impact of resource consumption attack on signal-stability based adaptive routing protocol in Manet. Indian Journal of Science and Technology. 2017 Aug;10:30.

[2] Medi Sandhya Rani, Rekha Redamalla and K.V.N. Sunitha “Secure Group Key Exchange and Encryption Mechanism in MANETs” in Innovations in Computer Science and Engineering, 2019

[3] Wan AnXoing and Yao Huan Gong, “Secure and Highly Efficient Three Level Key Management Scheme for Manet”, Wseas Transactions on Computers, Vol. 10, No. 10, 2011

[4] Khalili, Katz, Jonathan and Arbaugh, A. William, "Towards secure key distribution in truly ad hoc networks", IEEE Workshop on Security and Assurance in ad hoc Networks –2003.

[5] Néstor J. Hetnández Marcano, Jonas Gabs Fugl Nørby, and Rune Hylsberg Jacobsen, "On Ad hoc On-Demand distance vector routing in low earth orbit nanosatellite constellations", In IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, pp. 1-6, 2020, 10.1109/VTC2020-Spring48590.2020.9128736.

[6] Rajashanthi, M., and Valarmathi K, "Energy-efficient multipath routing in networking aid of clustering with OGFSO algorithm", Soft Computing, pp. 1-10, 2020, 10.1007/s00500-020-04710-4.

[7] Muthukumaran, N, "Analyzing throughput of MANET with reduced packet loss", Wireless Personal Communications, vol. 97, no. 1, pp. 565-578, 2017.

[8] Yimin Lv, "Security Issues in Multi-hop Device-to-device Communication Networks - Secure Routing Protocols Solution" in Journal of Physics: Conference Series 1828 (2021) doi:10.1088/1742-6596/1828/1/012117

[9] Y. Prasad1 and R. Balakrishna, "Energy Efficient and Secured Clustering Algorithm using Fuzzy Logic with K-means Method in MANET" in Indian Journal of Science and Technology, Vol 12(19), DOI: 10.17485/ijst/2019/v12i19/144195, May 2019.

[10] Burmester, M. and B.D. Medeiros, 2009. On the security of route discovery in MANETs. IEEE Trans. Mobile Comput., 8: 1180-1188. DOI: 10.1109/TMC.2009.13

[11] Shu, T., M. Krunz and S. Liu, 2010. Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE Trans. Mobile Computing, 9: 941-954. DOI: 10.1109/TMC.2010.36

[12] Ahmadzadeh, S.A., S.A. Motahari and A.K. Khandani, 2010. Signal Space Cooperative Communication. IEEE Trans. Wireless Communication, 9: 1266-1271. DOI: 10.1109/TWC.2010.04.090059.

[13] Mohindra Ar, Gandhi C, A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET. Walailak J Sci & Tech [Internet] 2021Mar.9 DOI: https://doi.org/10.48048/wjst.2021.8987.

[14] Manjula T, Anand B. A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network. Journal of Ambient Intelligence and Humanized Computing. 2021.

[15] Wan An Xoing and Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for Manet", Wseas Transactions on Computers, Vol. 10, No. 10, 2011.

[16] Rajesh Kumar Dangi, Rachna Singh Thakur, Neha Rahinj, Sankalp Rajora & Dinesh Thakur, "Key Distributed Cryptography using Key Algorithm in MANET" in International Journal of Recent Advances in Engineering & Technology (IJRAET) ISSN (Online): 2347 - 2812, Volume-5, Issue -12, 2017.

[17] Vinitha. R. G "An Improved Efficient Data Transmission using Key Management in Mobile Ad-Hoc Network" in International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 RTICCT – 2017.

[18] Nitika Singhi and Ravi Singh Pippal "Analysis of Key Management Schemes in MANET" in International Journal of Applied Environmental Sciences ISSN 0973-6077 Volume 13, Number 2 (2018), pp. 161-169.

[19] Bing, Jie Wu and Yuhong Dong, "An efficient group key management scheme for mobile ad hoc network", International Journal and Networks, Vol. 2, No.3, 2008.

[20] K.Sanzgir, and B.Dahill, "A secure routing protocol for ad hoc networks", Proceeding of the 10th IEEE International Conference on Network Protocols, pp.1-10, 2000.

[21] Mr. Nikhil Surkar, Ms. Shriya Timande. (2012). Analysis of Analog to Digital Converter for Biomedical Applications. International Journal of New Practices in Management and Engineering, 1(03), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/6

[22] Vyas, A. ., & Sharma, D. A. . (2020). Deep Learning-Based Mango Leaf Detection by Pre-Processing and Segmentation Techniques. Research Journal of Computer Systems and Engineering, 1(1), 11–16. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/18