An Efficient Key Management Protocol for Group Security on MANET Routing

Bhawna Sharma
Department of Computer Science and Engineering,
MMEC, MM (Deemed to be University), Mullana, Ambala, India
bsbhawna90@gmail.com

Rohit Vaid
Department of Computer Science and Engineering,
MMEC, MM (Deemed to be University), Mullana, Ambala, India
rohit_vaid1@rediffmail.com

Abstract: Security in Mobile Adhoc Networks (MANETs) is most vulnerable area of concern due to its dynamic topology; centralize-less authority and shared wireless infrastructure. Group security using key management during communication is the area of consideration when communicating to a group. In this paper, anensemble of RSA and DH (Diffie-Hellman) algorithm is used for providing security during communication in group. This ensemble key management scheme is applied on AODV and performance is analysed using parameters like routing overhead, throughput and security level. After applying this algorithm, we have found that our proposedensemble methodreduces the routing overhead in different groups, improves the throughputapplying by varying the number of messagesand secure group communicationas compared to Diffie-Hellman. By combining RSA and DH the group security increased by 30% from the previousDiffie-Hellman.

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

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is a self-configuring system of smaller networks linked together for wireless communication. Every node in a MANET is free to follow its own path and, as a result, will change its links to other devices on a frequent basis [1]. Each node should encourage traffic that isn't related to its own usage, and act as a router. The most difficult challenge in constructing a MANET is ensuring that each node has the necessary information to correctly route traffic at all times. Such networks may be self-contained or connected to the widerinternet. In general, MANETs have a routable networking environment [2]. Specific features of MANET include the following: dynamic topology, multi-hop communication, decentralization infrastructure, scalability, and short connection. Security is a major challenge in group communication in MANETs due to its open nature.

Secure group communication is desired in many group oriented applications of mobile ad hoc network (MANET), and fruitful communication achieved only via trustable network environment[3]. In order to enhance the privacy among group members, proper group key management schemes can be used to encrypt and decrypt the payload. This management is serious task in flexible network like MANET due to dynamic node movement and limited available resources [4]. In order to get away from repeated group key refreshment for entire network, rekeying is done only in sub-networks, which is known as clusters.

The AODV protocol is a reactive protocol. Its method is hop-to-hop routing. A RREQ is sent by a node that wants to know the path to a certain receiver (Route Request). The intermediate nodes then forward the route request to the destination while simultaneously establishing a reverse route[5]. When the node receives a request with the path to the destination. It creates a Route Reply (RREP) that specifies the amount of nodes required to succeed in the destination. Each node that helps the source node to transmit this reply and establish a forward path to the destination node. The RREQ and RREP routing in the AODV protocol are depicted in fig 1. This is frequently a situation where the hop-by-hop route has been established from the source to the destination. AODV on-demand routing protocol and may be a reactive protocol. It's a minimalist behaviour since it doesn't overburden the ad hoc network and requires less memory than other protocols. It uses the IP protocol [6]. It constructs routes on-demand rather than maintaining a comprehensive list of routes for each destination[7].

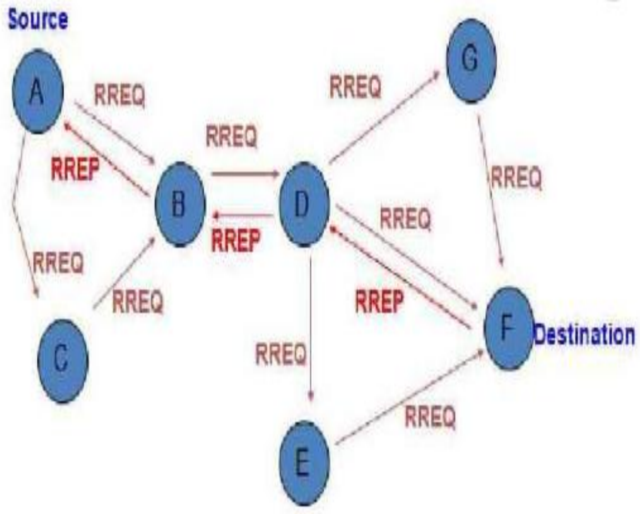

FIG. 1 RREQ AND RREP IN AODV [8]

AODV-efficient and Dynamic Probabilistic Broadcasting (EDPB) approach which is very effective and dynamic in nature and takes care of the communicate storm issue in AODV [9].

The rest of the paper is organized as follows: Section II discusses the related work. The description of key management is discussed in Section III, which covers an introduction to key management, secure group communication. Section IV dives into the proposed algorithm, experimental result is shown into section V. Finally, in Section VI, wrap up our work is presented.

II. RELATED WORK

Shu et al., [11] proposed randomized dispersive routes for wireless sensor networks for safe data collecting in MANET. It devised methods for generating randomizedmultipath routes. Burmesteret al., [10] created a QoS self-optimization in MANET for secure communication in a wireless ad-hoc network to deliver a satisfactory QoS (Quality of Service). The idea of signal space diversity is used to evaluate a single-hop transmitting system with a direct link between the source and the destination Ahmadzadeh et al., [12] highlighted difficulties and solutions for tradeoff between query processing in MANET by offering good services for secure data connection in order to provide a QoS service efficiently in MANET.

For Mobile ad hoc networks, Mohindraet al., [8] suggested a novel group key management protocol. They developed a well-organized key distribution approach for the password-authenticated group (also known as group key agreement) protocol, which is based entirely on multi-party Diffie Hellman group key exchange. The protocol's main goal is to create and distribute a secret session key, known as "K," among a group of nodes/customers who need to securely connect.

Manjula et al., [14], put for ad hoc networks, a group based on the scalable key management mechanism. Their procedure is described as a novel clustering methodology. Based on node affinity relationships, the network is organized into clusters. To ensure secure connections between nodes, they distributed two types of cluster head-generated keys. The protocol is adaptable to the battery power limitations of mobile nodes as well as dynamic topology changes. This suggested clustering method is based on a scalable key management system that ensures secure communication between ad hoc network nodes.

Wan et al., [15], suggested acluster-based security architecture for ad hoc networks.A distributed certification facility was presented, as well as a predictable security paradigm. Clusters are created in a network, each with its own unique head node [16]. These cluster head nodes functioned as organizational hubs and share a network key with other cluster members. Furthermore, for certification, a comparable key's used. In every cluster, simply one distinct node–the cluster head (CH)–is in rate of constructing and configuring the cluster [17].

III. KEY MANAGEMENT

In ad hoc networks, key management is difficult since it's hard to guarantee that a resource, Cryptography reduces the confidentiality and integrity of a communication to the confidentiality and integrity of a key (fig 2). In symmetric key cryptography, the nodes must agree on a secret key [13].The challenges are methods for establishing a secure key and re-keying it while minimizing storage and transmission overhead [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

There are two cases for secure communication- 1) communication between all the nodes, 2) Communication between selected nodes.

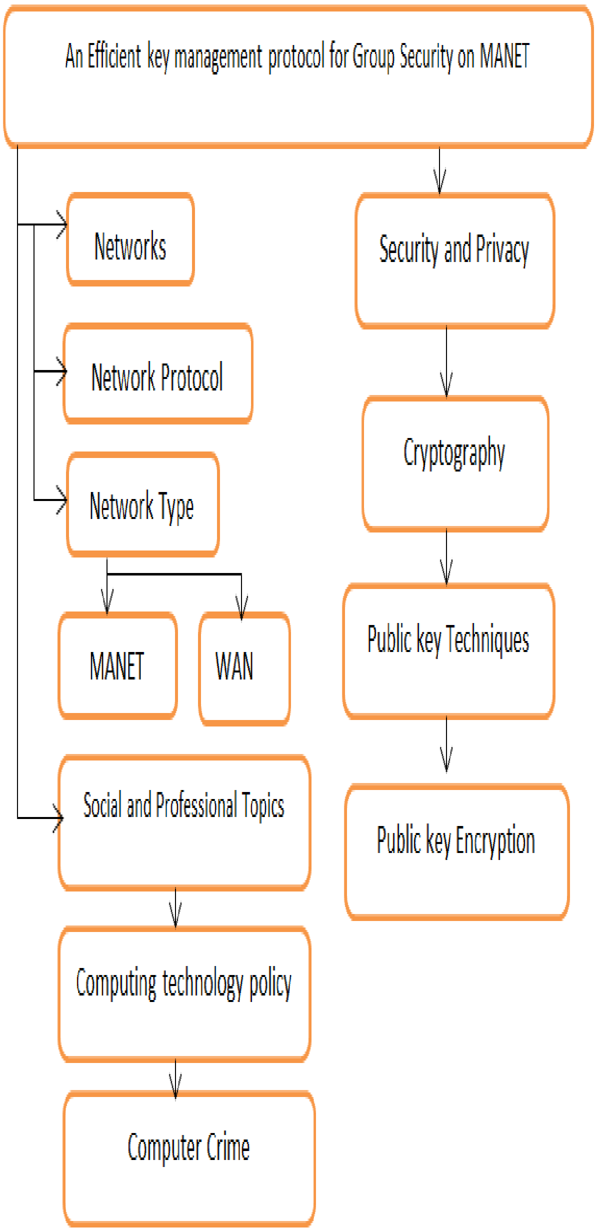

FIG.2 AN EFFICIENT KEY MANAGEMENT PROTOCOL FOR GROUP SECURITY ON MANET ROUTING PROTOCOL

1) Communication between all the nodes: In this communication, group member communicate with other nodes by encrypt the data with group key using symmetric key encryption algorithm. By using this algorithm data and group key considered as input and produce output which is known as cipher text. This cipher text decrypted by all the nodes using group key [18] as shown in fig 3.

2) Communication between selected nodes: In this communication when a node wants to communicate with other node in group, it encrypts the data with shared key using symmetric key encryption algorithm. This algorithm produces an output known as cipher text. For providing more security shared key encrypted with public key of the receiver. The receiver decrypts the shared key with its own private key [20] as shown in fig 4.

IV. PROPOSED ALGORITHM (RSA+DIFFIE HELLMAN)

Proposed Key interchange (RSA+Diffie Hellman)

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 = PT

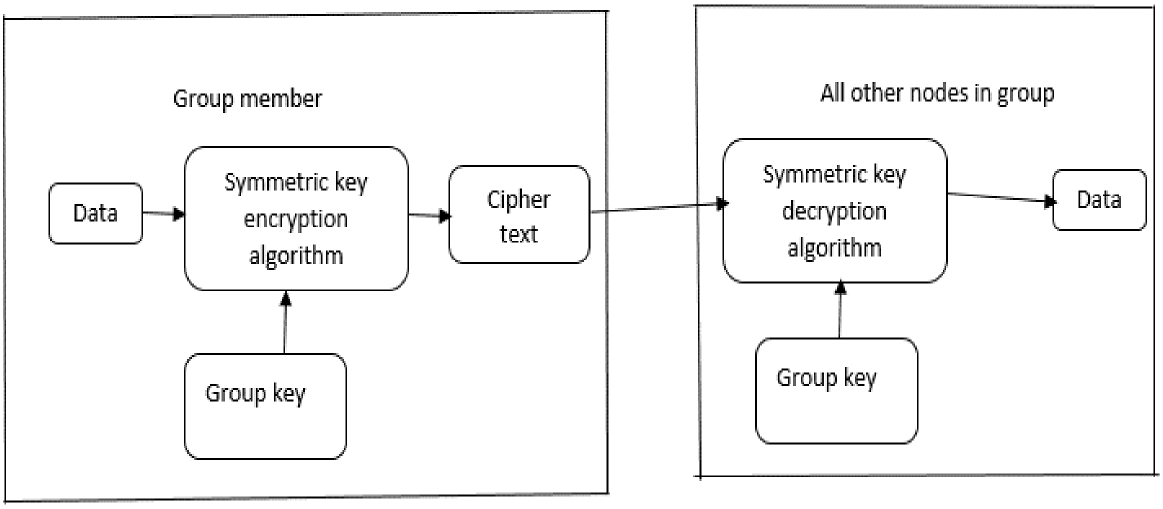

FIG.3COMMUNICATION BETWEEN ALL THE NODES

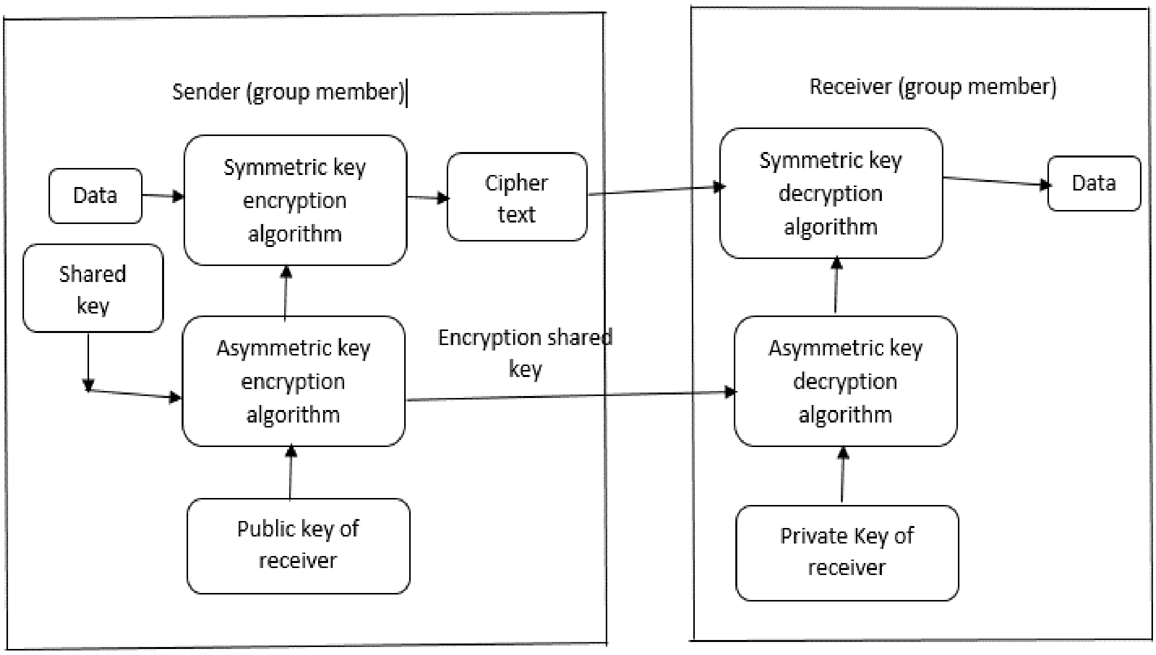

FIG.4COMMUNICATION BETWEEN SELECTED NODES

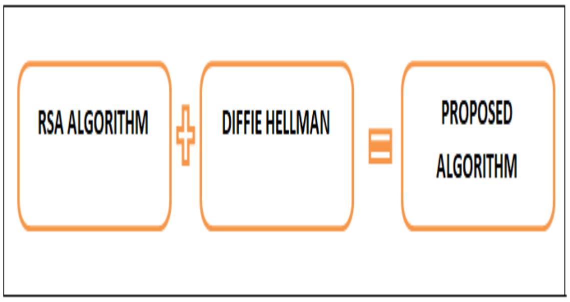

FIG.5 A PROPOSED ALGORITHM (RSA+DH)

Members of Security Group have exclusive access to their allowed data, and no other MANET group has access to data that is solely approved to that group. The group has a high level of security.New ways for resolving such challenges must be presented based on the survey conducted on routing mechanisms and key management approaches. A unique methodology for establishing effective routes in which data can be securely conveyed must be introduced .

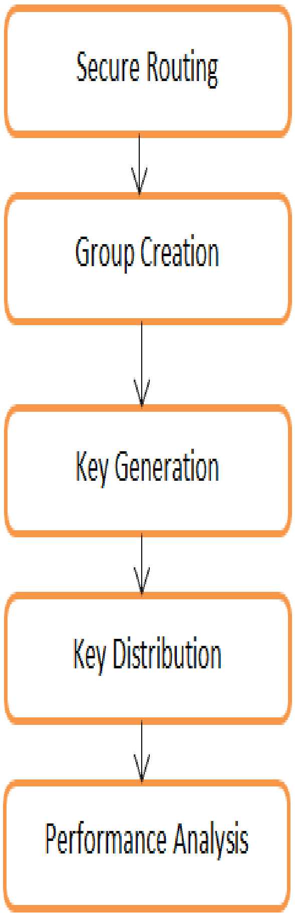

FIG. 6 PROPOSED FRAMEWORK

V. SIMULATION RESULTS AND ANALYSIS ON AODV PROTOCOL

The proposed method for Group security using Key Management is well-suited to a routing-based data security process in MANET, allowing for safe data communication AODV. In the NS-2 simulator, the proposed approach (RSA+DH) is implemented.

Routing overhead: Because MANET has a dynamic topology, there is a potential that a member of a group will leave it. As a result, the members' area keys may be changed when applying (RSA+DH) to that group.Rekeying overhead occurs at the moment of movement. When a member departs the MANET's domain, there is a higher rekeying overhead.

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

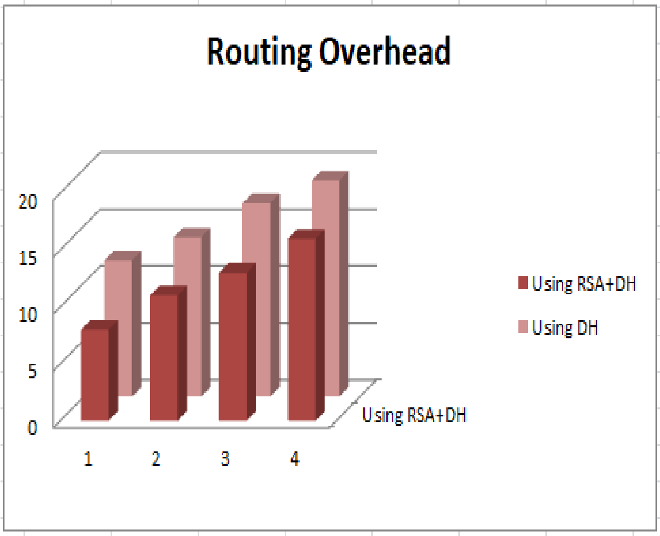

FIG. 7 NO. OF GROUPS TO THE ROUTING OVERHEAD

Using the suggested method, the process of routing overhead originating in secure groups formed in AODV in MANET is represented in Fig. 6.The proposed solution has a lower risk of routing overhead. Because the packet data is conveyed using a data security process in the suggested technique (RSA+DH), there is reduced probability of routing overhead. Fig7 depicts the proposed method's performance in terms of routing overhead. When compared to current approach, the proposed methodology would reduce routing overhead by 12-24 percent when routing packet data from source to destination (DH).

Throughput: It is defined as the average rate of successful message transmission from one group to another in MANET communication. The most common unit of measurement for power is bits per second (bps), however it can also be measured in packets per second or packets over time.The throughput in percentages for successful message transmission via MANET is shown in Table 2.

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

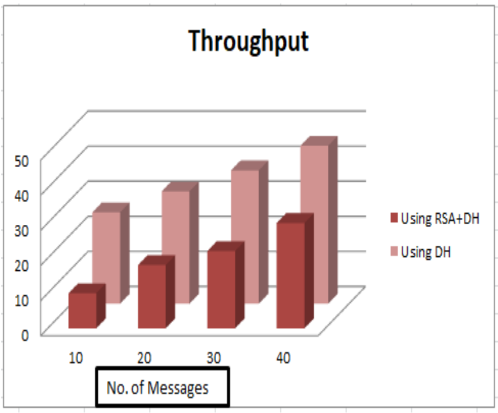

FIG. 8THE RATIO OF THE NUMBER OF MESSAGES IN GROUPS TO THE THROUGHPUT

The throughput for effective message delivery during a MANET using the new technique (RSA+DH) is shown in Fig 8.Since the group has been established as securely utilize keys in MANET, the proposed technique contains a high deliver rate of packet data. The packet data is conveyed using data security during this technique, and therefore the routing discovery step is performed first.

The proposed method's throughput performance is presented here. When compared to an existing DH, the proposed approach would have almost 80% higher variance in packet or data delivery throughput from source to destination. See Table 3.

TABLE 3: GROUP SECURITY LEVEL IN MANET

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

VI. CONCLUSION

For Mobile ad-hoc networks, key management using RSA+DH for group security provide superior performance. As a result, clustering nodes in AODV improves network productivity and efficiency with minimal overhead and increased network traffic. As a result, group-based networks can attain good scalability. The performance has been analyzed by using to different parameters – routing overhead, throughput and also measured the security level. After applying ensemble (RSA+DH) algorithm, we have found that our proposed method reduces the routing overhead and improves the throughput that is rate of successfully received packet has been increased and provide security which is about 80% secure as compared to normal DH method.In future we will extend this technology by including real-time data processing and transmission options.

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] MediSandhya Rani, RekhaRedamalla 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. HetnándezMarcano, Jonas Gabs FuglNørby, 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] YiminLv, "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] MohindraAr, Gandhi C, A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET. Walailak J Sci&amp; 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 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.

[16] Rajesh Kumar Dangi, Rachna Singh Thakur, NehaRahinj, SankalpRajora& 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] NitikaSinghi 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.