ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2022.0404

FOUR STAGE SECURITY ALGORITHM FOR DATA TRANSFER TO IMPROVE SECURITY IN MANET

C. Chandra Prabha[1] and Krishnaveni Sakkarapani[2]
[1]*Department of Computer Science, Pioneer College of Arts and Science, India*
[2]*Department of Computer Science, PSGR Krishnammal College for Women, India*

Abstract

Mobile Ad hoc Network (MANET) regarded to be a group of mobile nodes that can communicate with others in the absence of network infrastructure. MANET is at high risk due to its basic features, such as peer-to-peer (P2P) architecture; wireless shared medium, strictly constrained resources, extremely powerful network topology and open nodes for physical capture. Security is an essential service in all types of network communication. MANET must present security that raises human's belief in MANET. This paper proposed the Four Stage Security Algorithm (FSSA) improve MANET security. First, secret key-based encryption and decryption provided in Stage 1. Then, public key-based encryption and private key based decryption provided in Stage 2. Followed by, signature generation and verification provided in Stage 3, at last, token-based access control provided in Stage 4. The experimental result shows the proposed FSSA algorithm provides robust security compared with other existing algorithms in MANET.

Keywords:

Security, Cryptography, Encryption, Decryption, Access Control, Signature Generation and Verification

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is an integrated wireless device network that connects via bandwidth controlled wireless connections [1]. Each wireless device could serve as a sender, recipient and router. When a device is a sender, it could transmit packets to any particularized destination device by a specific route. As a recipient, it could receive packets from other nodes. When a device acts as a router, it could transmit a message to the destination and the next router in the path. If needed, each device could detect packets waiting to be shipped. Nodes randomly change position; therefore, at a given time, an ad hoc network available between the nodes, resulting in the formation of an arbitrary network. MANETs could be powerfully built within any collection of wireless customers and do not require an available framework.

Security on the Mobile Ad-Hoc Network (MANET) is critical to the basic functionality of the network [2]. Availability, confidentiality and data integrity of network services could attain by ensuring that security problems met [3]. Security threats frequently plague MANET because of attributes such as free media, altering its position, lack of central surveillance and administration, co-operation methods and no transparent security approach [4]. These elements have altered the battlefield circumstances for MANET in opposition to security threats.

Many security resolutions, cryptographic methods and key management planned to assist MANET. A few planned to meet network necessities (the smallest amount of latency, the smallest amount of energy expenditure and the largest amount of throughput), while others are computationally requiring. Cryptography plays an important role in concealing data [5], [6]. These encryption algorithms separated into two types as symmetric and asymmetric key cryptography algorithms [7]. Furthermore, the symmetric algorithm utilizes a similar key for encrypting and decrypting data. These once more separated into the stream and block ciphers. Block encryptions utilize data blocks for encryption and decryption, such as AES [8], [9], DES, and Blowfish. Stream ciphers utilize one bit at a time, such as RC4 [10]. In asymmetric key cryptography, two various keys utilized for encryption and decryption, one is the private key, and then another one is the public key. We could utilize one key for encryption and another for decryption such as the RSA algorithm. The public key is public, but the customer uses only the private key for decryption. Asymmetric algorithms are very slowly than symmetric key cryptography because of the huge processing of keys [11]. These algorithms utilize substantial computer resources like energy and bandwidth.

Therefore, this paper proposed the Four Stage Security Algorithm (FSSA) improve MANET security. This algorithm uses symmetric cryptography in stage 1, asymmetric cryptography in stage 2, signature generation and verification in stage 3, and token-based access control in stage 4. Compared with existing algorithms, this FSSA algorithm can improve MANET security efficiently.

The rest of the paper organized as follows: Section II provides a related work of previous cryptography, signature generation and verification and access control techniques. Section III presents the Four Stage Security Algorithm in comprehensive. Section IV presents broad experimental results to show the proposed FSSA algorithm performance. At last, Section V presents the conclusion of the work.

2. RELATED WORK

Public String Based threshold cryptography (PSTC) proposed by Chauhan et al. [12]. This project is implemented and simulated in ns-2. Since the program is based on trust value and analyzes denial of service attack, the node detects the attacker and rejects all messages from the attacker.

Joshi et al. [13] reported a technique of protecting MANETs based on hybrid cryptographic technology that utilizes the RSA and AES algorithm with the SHA 256 hashing mechanism. This hybrid cryptographic technology presents authentication for data.

Gupta et al. [14] developed the identity Based deniable authentication (IBDA) protocol accompanied by sufficient safety and performance. The suggested IBDA protocol primarily planned for MANET, where mobile devices are resource-constrained. The suggested IBDA protocol utilized identity-based cryptosystem (IBC) and elliptical curve cryptography (ECC).

Ahmed et al. [15] suggested the Secure Optimized Link State Route (SOLSR) protocol to compensate for security breach when adding message authentication code (MAC) value to find the path (s) from source to target, the signature. Subsequently, the encryption and global secret key in Hello Messages and Topology Control (TC) messages.

Deryabin et al. [16] proposed that MANET should ensure the authenticity and safety of contacts using the Redundant Residue Number System (RRNS). This method is eminent by its adaptable that is capable of controlling data honesty and enabling computational safe secret distribution using a residual number system (RNS).

Mohsen et al. [17] presented a key sharing method for the clustered ad-hoc networks. The network separated into clusters, and every cluster leader is in charge of sharing made more modern safety keys between cluster members and securing secrecy via encryption occasionally. Furthermore, an authentication method presented to guarantee the privacy of novel members to a cluster.

Kadim et al. [18] proposed symmetric cryptography to present confidentiality for the data packet by presented altered AES using the five presented which are: key generation using multiple chaotic methods, novel SubByte, novel ShiftRows, add-two-XOR, add-Shiftcycl.

Umar et al. [19] objective to integrate the previous co-operative bait discovery program that utilizes the baiting technique to bait malicious nodes into send a false path response and then use the reverse tracking function to discover malicious nodes. The packet first encrypts based on RSA algorithm before sending to the target to prevent eves trapper and other malicious nodes from unauthorized reading and writing in the data packet.

Usmani et al. [20] survey the gateway detection program with and without security based on various effective parameters such as packet delivery rate, end-to-end delay, routing overhead and throughput, then decide which is best.

Liu et al. [21] proposed B4SDC, a blockchain technique for collecting data associated with safety on MANETs. By managing the amount of RREQ sharing in path detection, the collector could control its fees and receive as many rewards as possible to guarantee that everyone who sends control data at the same time (i.e. RREQs and RREPs) is fair.

Ponguwala et al. [22] proposed the Energy Efficient Secure Routing (E2-SR) program to make sure data safety and truthfulness in MANET-IoT. The authors modify the certificate-based authentication in the Hash Chain-based Certification Authority (HCCA) program. Cluster generation involves the safe confirmation of IoT devices by elliptical curve panel legal formulas.

Satyamurthy et al. [23] are trying to integrate a novel technique in CEAACK MANETs by developing a cryptographic method to deal with the vulnerability of the network. This cryptography is very safe; it utilizes a unique assorted digital key that could be energetically created based on the Advanced Encryption Standard (AES) algorithm.

Ye et al. [24] presented the Distributed and Adaptive Hybrid Medium Access Control (DAH-MAC) technique for single-hop Internet of Things (IoT). This mobile ad hoc network supports voice and data services. A hybrid super frame system planned to accommodate packet transfers from different mobile nodes, creating latency-sensitive voice traffic or better effort data traffic.

Kwon et al. [25] provided random access congestion control techniques that use flexible management of random distribution and synchronization intervals. The simulation outcomes of the crowded urban junction demonstrate which the techniques significantly raise the success rate of security messages compared to WAVE CSMA / CA.

Jagannath et al. [26] presented an application-based opportunistic three-way handshake technique to negotiate medium access. The node selects the optimum transmission field, for example, the “direction” that increases the probability of initiating a connection even when a few of the neighbours suffer from deafness or blockage.

Li et al. [27] provided a scheme named DAPV that could detect single or collective malicious nodes and irregularly functioning paralyzed nodes. DAPV could discover straight and indirect attacks initiated during the routing stage.

Vinayagam et al. [28] presented a cross-layer technique to discover malicious devices in MANET. The authors are developing a cross-layer data tracking procedure to associate MAC (Media Access Control) layer parameters accompanied by network layer parameters to detect malicious devices from the network successfully.

Chen et al. [29] presented a novel technique of resource for file copying that considers both encounter frequency and node storage. The authors practically research the impact of resource allowance on mean query delay and obtain resource allowance rule to reduce mean query delay.

Narayana et al. [30] presented a cryptographic plan for creating keys and several routing algorithms for dynamic routing. An ad hoc on-demand distance vector (AODV) protocol is utilized that discovers the shortest route and creates the nodes obtainable for data transfer.

Alapathy et al. [31] presented a robust cryptographic system that creates and keeps keys and distributes keys securely to reliable nodes without malicious nodes. The presented system discovers malicious nodes and prevents involvement in communications from enhancing the packet distribution ratio and decrease network latency.

Vanathi et al. [32] presented a hyper-elliptical curve cryptography structure using signcryption for the key escrow. Here the model of the method is to separate a huge category into a lot of subgroups, each of which maintains its secret subgroup keys to managing the subgroup and manages multiple subgroups using the key escrow-based hyperelliptic curve cryptography management algorithm.

Asikka et al. [33] presented safe - efficient transfer (SET) to the versatile cluster-based Collection Key Protocol (SGKP) in MANET systems. At the proposed conference, the authors depict the elements that determine a novel, safe cluster head.

Mohindra et al. [34] create a novel scheme, the Secure Cryptography Based Clustering Mechanism (SCCM) for MANET. It includes the subsequent steps: Secure routing, encryption, signature creation, signature verification, and decryption.

Singanjude et al. [35] presented Identity-based cryptography is utilized alongside visual cryptography. In cryptography, which is mainly using identity, the RSA cryptography utilized to create public and private keys based on ancient Indian mathematics for rapid mathematical computation. RSA is a very safe and common algorithm. The authors in [37] performed an analysis on homomorphic technique for data security in fog computing. A lightweight authentication and secure data access between fog and IoT user was proposed in [38].

3. FOUR STAGE SECURITY ALGORITHM

This section proposed Four Stage Security Algorithm (FSSA) improve the security in MANET explained in Algorithm 1 and Fig.1. Each source mobile device wants to send data to the destination mobile device. After creating a message, the source mobile device encrypts a message based on a secret key. This encryption provides ciphertext 1 (Stage 1 Security) (Step 1 - 5). Followed by, it encrypts ciphertext1 based on the public key; this encryption provides ciphertext 2 (Stage 2 Security) (Step 6). Followed by, it generates a signature 1 for ciphertext2 based on token 1 (Stage 3 Security) (Step 7 - 8). Then send this (ciphertext 2 with token 1 with signature 1) as a single packet to destination mobile device via minimum power consumption routing (Stage 4 Security) (Step 9 - 10). After receiving this packet, the destination mobile device to enter a token of source mobile device is necessary.

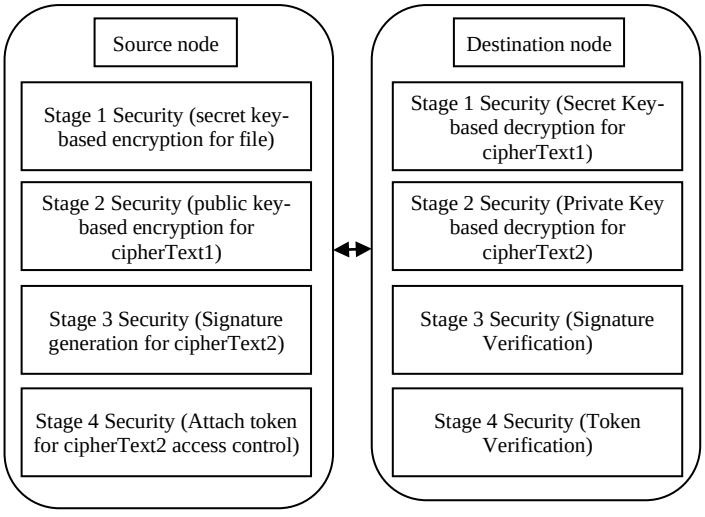

Fig.1. FSSA: Four Stage Security Algorithm Architecture

After destination mobile node enters source mobile device token (token 2), this packet splits (ciphertext 2 with token 1 with signature 1) separately. Then checks both token1 and token 2 is equal or not (Step 16). If both are equal destination mobile device is valid (Step 17) otherwise invalid (Stage 4 Security) (Step 31). Followed by destination mobile device generates a signature 2 for ciphertext2 based on token 2. Then checks both signature1 and signature2 are equal or not (Step 20). If both signatures are same, the received ciphertext 2 is safe (Step 21) otherwise modified by any hacker/attacker (Stage 3 Security) (Step 29). Followed by, the destination mobile device decrypts ciphertext2 based on the private key (Step 22). This decryption provides ciphertext 1 (Stage 2 Security). Furthermore, the destination mobile device decrypts ciphertext1 based on the secret key. This decryption provides original message (Stage 1 Security) (Step 23 - 27).

Algorithm 1: Four Stage Security Algorithm

Input: A source node (S), destination node (D), File (F), Public Key (PubKey), Private Key (PrivKey), Secret Key (SecKey), Token (Tok)

Output: Four Stage Security

SOURCE NODE SIDE

Stage 1 Security (secret key-based encryption for file)

1 : Cipher = Cipher.getInstance("AES")
2 : aesCipher.init(Cipher.ENCRYPT_MODE,SecKey)
3 : byteDataToEncrypt = F.getBytes()
4 : byteCipherText = aesCipher.doFinal(byteDataToEncrypt)
5 : cipherText1 = new BASE64Encoder().encode(byteCipherText)

Stage 2 Security (public key-based encryption for cipherText1)

6 : cipherText2 = Encryption(cipherText1, PubKey) // Algorithm 2

Stage 3 Security (Signature generation for cipherText2)

7 : sg = new Signature();
8 : signature1 = sg.calculateRFC2104HMAC(cipherText2,"HmacSHA1");

Stage 4 Security (Attach token for cipherText2 access control)

9 : packet = cipherText2 + "#" + signature1 + "#" + Tok;
10 : Send packet to a destination via Minimum Cost Routing Path

DESTINATION NODE SIDE

11 : sp[] = packet.split("#")
12 : cipherText2 = sp[0]
13 : signature1 = sp[1]
14 : Tok = sp[2]

Stage 4 Security (Token Verification)

15 : enteredToken = Enter token for verification
16 : IF enteredToken == Tok
17 : // Entered token is valid! So D can access this file!

Stage 3 Security (Signature Verification)

18 : sg = new Signature();
19 : signature2 = sg.calculateRFC2104HMAC(cipherText2,"HmacSHA1");
20 : IF(signature2 == signature1)
21 : // Signature is valid! So D can access this file!

Stage 2 Security (Private Key based decryption for cipherText2)

22 : cipherText1 = Decryption(cipherText2, PrivKey) // Algorithm 3

Stage 1 Security (Secret Key-based decryption for cipherText1)

23 : byteChipherText[] = new BASE64Decoder().decodeBuffer(cipherText1)
24 : aesCipher1 = Cipher.getInstance("AES")
25 : aesCipher1.init(Cipher.DECRYPT_MODE,SecKey,aesCipher1.getParameters())
26 : byteDecryptedText[] = aesCipher1.doFinal(byteChipherText)
27 : F = new String(byteDecryptedText)
28 : ELSE
29 : // Signature is invalid! So D cannot access this file!
30 : END IF
31 : // Entered token is Invalid! So D cannot access this file!
32 : END IF

3.1 ENCRYPTION

A source node needs to broadcast a message to the destination node. For safety, it encrypts a message based on its public key. This encryption algorithm discussed in Algorithm 2. This algorithm takes a cipherText1 and PubKey for input. Then it extracts e1 and m1 from PubKey (Step 1). Followed by, it gets cipherText1 into a character array (Step 2). Subsequently, it gets

each character (Step 4) and encrypts using a formula it mentioned in (Step 5). This encryption presents Ci. After combining all Ci, this algorithm presents cipherText2 (Step 6).

Algorithm 2: Encryption

Input	**:**	cipherText1, PubKey
Output	**:**	cipherText2
Step 1	**:**	Extract e1, m1 from PubKey
Step 2	**:**	CH[] = Convert cipherText1 into Character Array
Step 3	**:**	cipherText2 = {}
Step 4	**:**	For each character chi in CH
Step 5	**:**	Ci = CH^e1 mod m1
Step 6	**:**	cipherText2 = cipherText2 + Ci
Step 7	**:**	End For

3.2 DECRYPTION

After getting cipherText2 from the source node, the destination node decrypts it using PrivKey. Decryption procedure discussed in Algorithm 3. This algorithm gets cipherText2 and PrivKey as input. After that, it takes outs of e2 and m1 from PrivKey (Step 1). From cipherText2, this algorithm take-outs all Ci (Step 2). Subsequently, it gets each Ci (Step 4) and decrypts using a formula it is declared in (Step 5). This decryption presents Orig. After combining the entire Orig, this algorithm presents cipherText1 (Step 6).

Algorithm 3: Decryption

Input : cipherText2, PrivKey
Output : cipherText1
Step 1 : Extract e2, m1 from PrivKey
Step 2 : Cis[] = Extract all Ci from cipherText2
Step 3 : cipherText1 = {}
Step 4 : For each Ci from Cis
Step 5 : Orig = Ci^e2 mod m1
Step 6 : cipherText1 = cipherText1 + Orig
Step 7 : End For

4. EXPERIMENTAL RESULTS

This section presents the experimental outcomes and study of Four Stage Security Algorithm (FSSA) in MANET. For experimental analyzes, randomly created networks utilized. This simulation presumes that 100 mobile devices uniformly and randomly spread in a 900 m × 600 m unit region. Radio propagation range for each device is 100 m and devices initial energy is 100 J chosen—the data payload size allocated as 512 bytes. To assess the FSSA algorithm java utilized. For assess cryptography algorithm, evaluate proposed FSSA algorithm accompanied by various well-known cryptography algorithms for example DES [11], AES [8], Blowfish [12], RC4 [17], TBSA [18], Camellia [19], CAST-128 [19], SEED [19] and AKCSS [36] in terms of the energy consumption.

Energy consumption details of Each cryptography algorithm shown in Table.1.

Table.1. Comparison of Various Cryptography Algorithms using Power Expenditure

Algorithm	Power Expenditure (in microjoule)
DES	2.80
AES	1.20
Blowfish	0.81
RC4	0.49
TBSA	0.20
AKCSS	0.02692
FSSA	0.01982

Power expenditure details of each cryptography algorithm demonstrated in Table.1. Table 2 demonstrates the encryption time comparison of various cryptography algorithms based on message size correspondingly 100, 500, 1000 and 2000 bits.

Table.2. Comparison of Various Cryptography Algorithms using Encryption Time (in microseconds)

Message Size (in bits)	DES	AES	Blow fish	Camel lia	CAST-128	SEED	AKCSS	FSSA
100	22	15	9	46	20	20	2	1
500	50	32	23	226	42	54	12	10
1000	90	45	42	400	76	88	33	29
2000	194	91	88	802	183	206	82	78

Compared with DES, AES, Blowfish, Camellia, CAST-128, SEED and AKCSS, this proposed FSSA algorithm takes a smaller amount of time for encryption is demonstrated by Fig. 3.

Fig. 3: Comparison of Various Cryptography Algorithms using Encryption Time (in microseconds)

Table 2 demonstrates the decryption time comparison of various cryptography algorithms based on message size, respectively 100, 500, 1000 and 2000 bits.

Table.3. Comparison of Various Cryptography Algorithms using Decryption Time (in microseconds)

Message Size (in bits)	DES	AES	Blow fish	Cam ellia	CAST-128	SEED	AKCSS	FSSA
100	5	16	4	3	11	14	2	1
500	38	39	20	18	33	42	16	13
1000	69	63	38	36	61	86	23	19
2000	134	120	82	60	121	164	53	49

5. CONCLUSION

This paper proposed a Four-Stage Security Algorithm (FSSA) Algorithm to improves security in MANET. In MANETs, a well-organized safety technique using efficient encryption and

decryption technique that can accomplish entire vital data safety necessities and use a smaller amount of power for data encryption well required. In this paper, a safety algorithm, that is to say, FSSA, using easy and proficient encryption, access control, signature generation and verification process implemented. First, secret key-based encryption and decryption provided in Stage 1. Then, public key-based encryption and private key based decryption provided in Stage 2. Followed by, signature generation and verification provided in Stage 3, at last, token-based access control provided in Stage 4. The experimental outcomes verified that FSSA algorithms present assured lifespan via less power expenditure when data transfer in MANET.

REFERENCES

[1] M. Elhoseny, K. Shankar, "Reliable Data Transmission Model for Mobile Ad Hoc Network using Signcryption Technique", *IEEE Transactions on Reliability*, Vol. 69, No. 3, pp. 1077-1086, 2019.

[2] P. Sathyaraj and D.R. Devi, "Designing the Routing Protocol with Secured IoT Devices and QoS over Manet using Trust-Based Performance Evaluation Method", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 30, pp. 1-9, 2020.

[3] M.S. Pathan, N. Zhu, J. He, Z.A. Zardari, M.Q. Memon and M.I. Hussain, "An Efficient Trust-based Scheme for Secure and Quality of Service Routing in MANETs", *Future Internet*, Vol. 10, No. 2, pp. 1-16, 2018.

[4] R. Menaka, V. Ranganathan and B. Sowmya, "Improving Performance through Reputation based Routing Protocol for Manet", *Wireless Personal Communications*, Vol. 94, No. 4, pp. 2275-2290, 2017.

[5] V.L. Narayana and C.R. Bharathi, "Identity based Cryptography for Mobile Ad Hoc Networks", *Journal of Theoretical and Applied Information Technology*, Vol. 95, No. 5, pp. 1173-1183, 2017.

[6] J. Sultana and T. Ahmed, "Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET", *International Journal of Electrical and Computer Engineering*, Vol. 8, No. 6, pp. 1-17, 2018.

[7] S. Khatoon and B.S. Thakur, "Certificate Less Key Management Scheme in Manet using Threshold Cryptography", *International Journal of Network Security and Its Applications*, Vol. 7, No. 2, pp. 55-63, 2015.

[8] B. Xing, D. Wang, Y. Yang, Z. Wei, J. Wu and C. He, "Accelerating DES and AES Algorithms for a Heterogeneous Many-Core Processor", *International Journal of Parallel Programming*, Vol. 49, No. 3, pp. 463-486, 2021.

[9] S.H. Hashem, "Proposal Hybrid CBC Encryption System to Protect E-mail Messages", *Iraqi Journal of Science*, Vol. 28, pp. 157-170, 2019.

[10] M.M. Abd Zaid and S. Hassan, "Lightweight RC4 Algorithm", *Journal of Al-Qadisiyah for Computer Science and Mathematics*, Vol. 11, No. 1, pp. 1-27, 2019.

[11] V. Bhardwaj and N. Kaur, "SEEDRP: A Secure Energy Efficient Dynamic Routing Protocol in Fanets", *Wireless Personal Communications*, Vol. 85, pp. 1-27, 2021.

[12] G.K. Chauhan and S.M. Patel, "Public String Based Threshold Cryptography (PSTC) for Mobile Ad Hoc Networks (MANET)", *Proceedings of International Conference on Intelligent Computing and Control Systems*, pp. 1-5, 2018.

[13] V.B. Joshi and R.H. Goudar, "Intrusion Detection Systems in MANETs using Hybrid Techniques", *Proceedings of International Conference on Smart Technologies for Smart Nation*, pp. 534-538, 2017.

[14] D.S. Gupta, S.H. Islam and M.S. Obaidat, "A Secure Identity-based Deniable Authentication Protocol for MANETs". *Proceedings of International Conference on Computer, Information and Telecommunication Systems*, pp. 1-5, 2019.

[15] M. Ahmad, Q. Chen, M. Najam-Ul-Islam, M.A. Iqbal and S. Hussain, "On the Secure, Optimized Link State Routing (SOLSR) Protocol for MANETs", *Proceedings of International Conference on Intelligent Systems and Knowledge Engineering*, pp. 1-8, 2017.

[16] M. Deryabin, M. Babenko, A. Nazarov, N. Kucherov, A. Karachevtsev, A. Glotov and I. Vashchenko, "Protocol for Secure and Reliable Data Transmission in MANET based on Modular Arithmetic", *Proceedings of International Conference on Engineering and Telecommunication*, pp. 1-5, 2019.

[17] Y. Mohsen, M. Hamdy and E. Shaaban, "Key Distribution Protocol for Identity Hiding in MANETs", *Proceedings of International Conference on Intelligent Computing and Information Systems*, pp. 245-252, 2019.

[18] H. Kadhim and M.A. Hatem, "Secure Data Packet in MANET Based Chaos-Modified AES Algorithm", *Proceedings of International Conference on Engineering Technology and its Applications*, pp. 208-213, 2019.

[19] M. Umar, A. Saba and A.A. Tata, "Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET", *Proceedings of International Conference on Networking and Network Applications*, pp. 121-126, 2018.

[20] J. Usmani, R. Kumar and J. Prakash, "A Survey on Secure Gateway Discovery in MANET", *Proceedings of International Conference on Cloud Computing, Data Science and Engineering*, pp. 362-368, 2017.

[21] G. Liu, H. Dong, Z. Yan, X. Zhou and S. Shimizu, "B4SDC: A Blockchain System for Security Data Collection in MANETs", *IEEE Transactions on Big Data*, Vol. 67, pp. 1-17, 2020.

[22] M. Ponguwala and S. Rao, "E2-SR: A Novel Energy-Efficient Secure Routing Scheme to Protect MANET-IoT", *IET Communications*, Vol. 13, No. 19, pp. 3207-3216, 2019.

[23] J. Sathiamoorthy, B. Ramakrishnan and M. Usha, "A Reliable and Secure Data Transmission in CEAACK MANETs using a Distinct Dynamic Key with a Classified Digital Signature Cryptographic Algorithm", *Proceedings of International Conference on Computing and Communications Technologies*, pp. 144-151, 2015.

[24] Q. Ye and W. Zhuang, "Distributed and Adaptive Medium Access Control for Internet-of-Things-Enabled Mobile Networks", *IEEE Internet of Things Journal*, Vol. 4, No. 2, pp. 446-460, 2016.

[25] T.H. Kwon, W. Jo, J.Y. Lee, HS. Seo, M. Baek and S.S. Lee, "Random Access Congestion Control for Periodic Safety Messages in Dense Traffic Networks", *Proceedings of*

International Conference on Computer Communication and Networks, pp. 1-4, 2019.

[26] J. Jagannath and T. Melodia, "An Opportunistic Medium Access Control Protocol for Visible Light Ad Hoc Networks", *Proceedings of International Conference on Computing, Networking and Communications*, pp. 609-614, 2018.

[27] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing with Provenance and Verification", *IEEE Access*, Vol. 7, pp. 35302-35316, 2019.

[28] J.K. Vinayagam, C.H. Balaswamy and K. Soundararajan, "Adopting a Cross-Layer Approach for Detecting and Segregating Malicious Nodes in MANET", *Proceedings of International Conference on Signal Processing and Communication*, pp. 457-461, 2017.

[29] K. Chen and H. Shen, "Maximizing P2P File Access Availability in Mobile Ad Hoc Networks through Replication for Efficient File Sharing", *IEEE Transactions on Computers*, Vol. 64, No. 4, pp. 1029-1042, 2014.

[30] V.L. Narayana and C.R. Bharathi, "Multi-Mode Routing Mechanism with Cryptographic Techniques and Reduction of Packet Drop Using 2ACK Scheme MANETs", *In Smart Intelligent Computing and Applications*, pp. 649-658, 2019.

[31] Y.K. Alapati and S. Ravichandran, "Secure Data Transfer in Manet with Key Calculator and Key Distributor Using Cryptography Methods", *International Information and Engineering Technology Association*, Vol. 10, No. 4, pp. 567-572, 2020.

[32] B. Vanathy and M. Ramakrishnan, "Signcryption Based Hyper Elliptical Curve Cryptography Framework for Key Escrow in Manet", *International Journal of Advanced Research in Engineering and Technology*, Vol. 11, No. 3, pp. 91-107, 2020.

[33] S.N. Asikka, "Authenticated Group Key Agreement Protocol for MANET Based on Cryptographic Techniques", *International Journal of Research in Engineering, Science and Management*, Vol. 13, No. 7, pp. 13-19, 2020.

[34] A. Mohindra and C. Gandhi, "A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in Manet", *Walailak Journal of Science and Technology*, Vol. 9, pp. 1-18, 2020.

[35] M.D. Singanjude and R. Dalvi, "Secure and Efficient Application of Manet Using RSA Using Vedic Method Combine with Visual Cryptography and Identity Based Cryptography Technique", *Proceedings of International Conference on Innovative Computing and Communications*, pp. 1-7, 2020.

[36] R. Preethi and M. Sughasiny, "AKCSS: An Asymmetric Key Cryptography Based on Secret Sharing in Mobile Ad Hoc Network", *Proceedings of International Conference on Intelligent Systems Design and Applications*, pp. 73-86, 2018.

[37] A. Murugesan, B. Saminatha, F. Al-Turjman and R.L Kumar, "Analysis on Homomorphic Technique for Data Security in Fog Computing", *Transactions on Emerging Telecommunications Technologies*, Vol. 39, pp. 1-14, 2020.

[38] A. Murugesan, B. Saminathan, F. Al-Turjman and R.L Kumar, "A Lightweight Authentication and Secure Data access Between Fog and IoT User", *International Journal of Electronic Business*, Vol. 16, No. 1, pp. 77-87, 2021.