Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9134036, 8 pages
https://doi.org/10.1155/2022/9134036

Research Article

Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System

Mohammad Sirajuddin[1], **Ch. Rupa**[2], **Surbhi Bhatia**[3], **R. N. Thakur**[4] and **Arwa Mashat**[5]

[1]*Department of Information Technology, Kallam Haranadhareddy Institute of Technology, Guntur, India*
[2]*Department of C.S.E., V.R. Siddhartha Engineering College, Vijayawada, India*
[3]*Department of Information Systems, College of Computer Sciences & Information Technology, King Faisal University, Al Hasa, Saudi Arabia*
[4]*LBEF Campus, Kathmandu, Nepal*
[5]*Faculty of Computing & Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh 21911, Saudi Arabia*

Correspondence should be addressed to R. N. Thakur; rn.thakur@lbef.edu.np

Received 4 February 2022; Revised 10 March 2022; Accepted 17 May 2022; Published 16 June 2022

Academic Editor: Kuruva Lakshmanna

The COVID-19 pandemic has affected people's lives in all aspects. This pandemic has raised the usage of ubiquitous networks such as mobile ad hoc networks (MANETs) for information exchange in various domains. MANET is a group of versatile nodes that communicates with each other without relying on a fixed physical framework. One of the prominent features of MANET is its versatile topology. Because of this striking feature, MANETs are employed in various domains like defense and combat operations, disaster management, healthcare, and environmental monitoring. In this paper, we enlighten the significance of MANET in the smart healthcare system. The COVID-19 pandemic outbreak demanded the reshaping of the healthcare systems to combat the pandemic and similar cataclysms. Existing healthcare systems are proved inefficient in dealing with pandemic situations, because they are not fully automated and also vulnerable to various security attacks. Therefore, it is vital to empower the healthcare sectors by integrating ubiquitous networks and other emerging technologies. In this paper, we proposed a MANET-based secure healthcare system to exchange medical data among portable nodes. Ensuring secure communication in the MANET-based healthcare system is one of the challenging issues. Healthcare system demands the sharing of confidential medical data among mobile nodes. So it is essential to provide secure information exchange in healthcare system by using strong cryptographic schemes. In this paper, we proposed a hybrid cryptographic algorithm for secure medical information exchange among mobile healthcare nodes. The proposed cryptographic scheme uses logistic map for key generation. Logistic map exhibits high security with less computational power. Our simulation results show that the proposed hybrid cryptographic scheme exhibits better security against various attacks in MANET-based healthcare systems.

1. Introduction

Mobile ad hoc network emerged as an illustrious wireless technology that allows nodes to communicate without relying on physical infrastructure and administrative support. The pandemic outbreak demanded the metamorphosis of traditional healthcare systems [1]. The traditional healthcare system involves the exchange of medical information among nodes that are connected via a physical network. However, some healthcare systems allow wireless devices to access and exchange medical data but they are highly susceptible to various security threats and breaches. In this paper, we proposed a secure MANET-based healthcare system for medical information exchange among portable healthcare

nodes. The mobile healthcare nodes are used for collecting and exchanging people's or patient's medical data. This collected medical data can be used further for analysis and disease predictions [2]. The swapping of data between heterogeneous mobile nodes invokes various security risks due to open communication channel [3]. Therefore, MANET-based healthcare systems are also susceptible to various attacks due to dynamic topology and openness of communication medium. Any malicious node may join the network easily and become part of it. The presence of malicious nodes has a significant impact on the performance of the network and also compromises the entire network [4]. Some security attacks that may be triggered in MANET-based applications are blackhole attack, grayhole attack, wormhole attack, jellyfish attack, DoS attack, etc. All these attacks degrade the performance of the network either by dropping legitimate packets or flooding the network by spurious packets thereby preventing access to service. So, it is necessary to implement security protocols to ensure secure information exchange among healthcare nodes. Secure information exchange among healthcare nodes can be accomplished by means of an authentication protocol and cryptographic schemes. The authentication protocol authenticates the mobile healthcare nodes at the time of joining the network and at same time prevents the malicious node(s) from joining the network. Furthermore, it is also necessary to design lightweight strong cryptographic schemes that consume less battery power of nodes. The lightweight cryptographic scheme must provide the confidentiality with the constrained resources of the network and nodes. In this paper, we proposed an authentication and hybrid cryptographic schemes for handling various attacks in the MANET-based smart healthcare system. The proposed healthcare network model allows mobile healthcare nodes to exchange medical data securely among themselves.

This paper is organized as follows. First, the related work is discussed in Section 2. In Section 3, we demonstrate the functionality of the proposed model and the methodology. In Section 4, we discuss the performance analysis of the proposed method by comparing it with the existing methods. Section 5 contains the conclusion part.

2. Related Work

This section enlightens various recent cryptographic approaches developed to address the security issue in the MANET. In our literature survey, we found that researchers considered the security aspect in two paradigms; one is the implementation of routing protocols by adding some security features to them and second is the implementation of cryptographic algorithms. Some routing protocols have been developed by integrating intrusion detection framework that executes necessary operations in mitigating attacks without using any specialized cryptographic approaches. We also studied various cryptographic algorithms designed for MANETs to provide authentication, data confidentiality, and message integrity. We outlined the description of some existing cryptographic techniques recommended for MANET-based applications.

Ahmad and Ismail [5] proposed user selective encryption method for providing security to the MANET. This contribution allows user to select a suitable cryptographic algorithm as demanded by MANET application and the level of security required. This research work demonstrated the performance of DES, 3DES, AES, and DHKE protocol by considering transfer time, throughput, number of hops, etc., through simulation in MANET.

Echchaachoui et al. [6] proposed OLSR-SDK protocol to improve the security of the system. This protocol implements key generation and distribution schemes by using specialized nodes called cluster heads. Moreover, this propounded scheme is based on asymmetric and dynamic encryption approach. This scheme is compatible with the OLSR routing protocol only.

Khan et al. [7] proposed a partial permutation encryption technique for network coded MANET. The main strength of this work is the key generation algorithm and random permutation confusion computation. Also, the use of partial permutation made this approach efficient in terms of energy, computation and space.

Hamamreh et al. [8] developed RAD protocol which uses MD5, Diffie-Hellman, and reinforcement approach for secure routing. In this approach, reinforcement learning is used to analyze the behaviour of nodes in MANET. This approach identifies and mitigates the malicious nodes from the network. MD5 is used to perform authentication between nodes, and the Diffie-Hellman technique is implemented to share secret keys among the nodes. This RAD protocol does not require any third party for secret key distribution. Moreover, this protocol avoids the selection of route which includes malicious nodes.

Vanathy and Ramakrishnan [9] demonstrated KEHECCS technique that uses signcryption approach based on hyperelliptic curve cryptography for key escrow. This KEHECCS technique supports the concept of group key management by using two algorithms called SSKG and GSKG. SSKG is used for sharing secret key whereas GSKG is used for group key sharing. This approach is compared with AES, DES, and ECC techniques. This propounded approach exhibits better throughput, storage cost, and communication overhead than the existing DES, AES, and ECC techniques.

Public key infrastructure (PKI) is also an extensively used identity authentication scheme in MANET-based applications. But this scheme has certain limitations like single point of failure and oppressive key management [3]. Some researches emphasized on identity-based batch verification schemes to facilitate the signing of messages and verification of the signature of messages in ad hoc networks. Many researchers focused on enhancing the efficiency of batch verification algorithms rather than improvising the identification of invalid signatures [2, 10–12]. Such batch verification schemes cause performance degradation. Table 1 outlines the functionalities of existing approaches that are considered in our literature study for identifying the research gaps. Many strong cryptographic algorithms have been proposed by many researchers for ensuring secure communication in MANET. But only limited work has been done in designing energy efficient cryptographic algorithms that enhance the lifetime of the network.

Many researchers are extending wireless sensor networks by integrating cutting-edge technologies like cloud

Table 1: Summary of related work.

Authors	Cryptographic approach	Security services	Key management	Key size	MANET routing protocol	Attacks considered	Performance metrics
Ahmad and Ismail [5]	Selective encryption approach (symmetric)	(i) Confidentiality	No	128 bits	AODV	—	(i) Encryption time (ii) Data transfer rate (iii) Throughput
Echchaachoui et al. [6]	Asymmetric	(i) Confidentiality	Yes	—	OLSR-SDK	(i) Blackhole attack (ii) DDOS attack	(i) PDR (ii) End-to-end delay
Khan et al. [7]	PPE scheme	(i) Confidentiality	Yes	32 bits	DSR	(i) Adversarial attack	(i) Throughput (ii) Encryption time (iii) Energy consumption
Hamamreh et al. [8]	RAD protocol (MD5 and DH)	(i) Authentication (ii) Confidentiality (iii) Data integrity	No	128 bits	DYMO	—	(i) Avg. throughput (ii) PDR (iii) End-to-end delay
Vanathy and Ramakrishnan [9]	KEHECCS	(i) Authentication (ii) Confidentiality	Yes	52 bits	—	(i) Key compromise attack	(i) Storage cost (ii) Communication overhead (iii) Throughput

computing, fog computing, and big data analytics to implement distributed healthcare applications [13, 14].

MANET-based frameworks with the convergence of cloud computing and IoT are extensively used to provide the finest healthcare services. Juneja et al. [15] proposed an IoMT-based healthcare infrastructure for diagnosing and treating diseases irrespective of physical locations of patients.

It is also important to optimize the energy consumption of wireless nodes or sensors to enhance the life span of the network. Wireless nodes are continuously involved in data generation and distribution. Such activities consume the battery power of nodes. So it is necessary to incorporate energy efficient techniques for network life management. Iwendi et al. [16] proposed WOA-SA approach to optimize the energy consumption of wireless sensors.

In this paper, we proposed a cryptographic algorithm that uses an asymmetric key cryptography approach along with the chaotic function for generating keys. The keys that are generated by using chaotic function are very difficult to crack by the intruders or attackers [17]. The chaotic signals are complex, random, and unpredictable. These properties make chaotic function suitable for key generation by supporting the property of confusion and diffusion. One of the striking features of chaotic function is that a small change in one control parameter results in a completely different pattern that makes the guessing of keys and plain text tedious for an attacker. The proposed security model ensures both data confidentiality and authentication by employing lightweight computations.

3. Proposed Methodology

In this paper, we proposed a MANET-based healthcare system model along with hybrid cryptographic scheme to ensure secure communication among healthcare nodes. The proposed network model is a derivative of SKG (Secure Key Generator) node-based security model [18]. This MANET-based healthcare system runs over trust-based I-AODV routing protocol [4, 18, 19]. In I-AODV, routing is performed based on the trust value of nodes. In this protocol, only trusted nodes are allowed exchange messages. Furthermore, the SKG-based routing protocol is extended in this paper by providing an efficient key generation approach along with the asymmetric key cryptographic scheme. We considered SKG node as a Master Healthcare Node (MHN) in our proposed model for ensuring authentication, key generation, and key distribution.

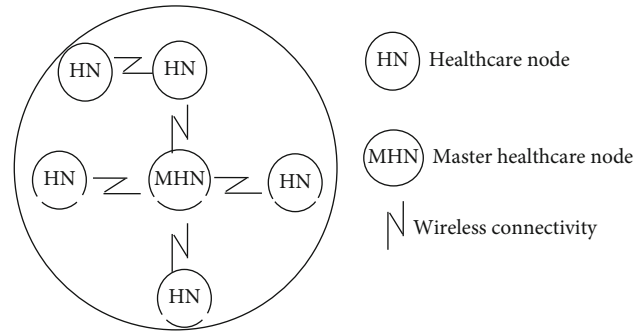

Figure 1: MANET-based healthcare network model.

3.1. Registration and Key Management. In this protocol, firstly, all the mobile healthcare nodes must register with the MHN node. The MHN node will authenticate all the registered healthcare nodes by providing them unique ID. Only registered healthcare nodes are allowed to participate in the routing process. A MHN node is responsible for monitoring the functionality of mobile healthcare nodes in the network.

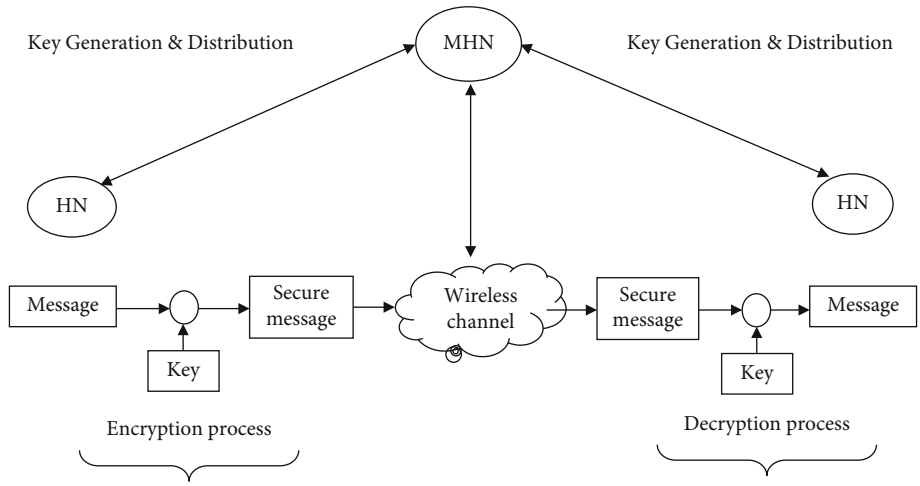

Figure 2: Proposed security model.

The structure of the proposed network model is depicted in Figure 1. The proposed model of cryptosystem is shown in Figure 2. In the proposed security model, a MHN node is responsible for key generation and distribution. Prior to information exchange, sender and receiver HN nodes must request for secret keys from MHN node. Once sender HN node receives secret key from MHN node, it encrypts the message and send encrypted message to the receiver. The receiver HN node decrypts the message by using the key received from MHN node. The proposed methodology also provides a mechanism to securely exchange keys between MHN node and HN nodes. Hence, it supports double security by using RSA and hybrid cryptographic approach compared to the existing approaches [16, 20, 21].

A node having the highest trust value, computational power, sophisticated battery power, and active in a network for a longer period of time will be selected as a MHN. The main purpose of this MHN is to generate a session key for every pair of sender and receiver. This key is used in the encryption and decryption process. After registration of nodes, each node uses RSA algorithm to generate a pair of keys called public key and private key. Whenever a sender node intends to send data to the receiver node, first it sends a request packet to the MHN for session key by using KREQ (KeyRequest) packet. After receiving the KREQ packet, MHN verifies the authenticity of the sender node and then generates a session key, i.e., SK, and stores it in memory. This session key (SK) will be sent in an encrypted format to the sender node. The sender node uses this SK during the encryption of plaintext. To generate this SK, the MHN node uses a chaotic function for making the keys difficult to guess by the intruders and also supports confusion and diffusion property. After receiving the encrypted message, the receiver node requests the MHN for the SK by sending a KREQ packet. After receiving the SK, the receiver node uses that key for performing the decryption operation. Figure 3 demonstrates the process of how the sender node and receiver node communicate with MHN for the session key.

The process of encryption and decryption is explained as follows.

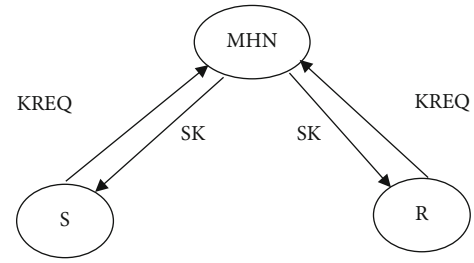

Figure 3: Key generation process.

3.1.1. Encryption Process

Step 1. RSA algorithm is used to generate public and private keys at sender node.

Step 2. Before sending data to the receiver, the sender node request session key (SK) from MHN node. MHN node generates the SK by verifying authenticity of sender and receiver nodes.

Step 3. To generate SK, MHN node uses logistic map function represented as

$$Z_{n+1} = rZ_n(1 - Z_n), \tag{1}$$

where r is a control parameter whose value ranges from $3.83 < r < 4.0$ and $Z\,e\,[0.0,1.0]$.

Step 4. Generate a sequence with selected r value, i.e., 3.99, and store that sequence of values in an array KS[].

Step 5. Randomly select one value from KS[] and store it in $K1$ variable.

Step 6. $K2 = \text{round}(K1 * \alpha)$, where α is some constant positive integer which is generated randomly by MHN node using random number generation function.

Step 7. Consider a seed value on which linear feedback left shift operation is performed.

Convert the seed value into binary sequence, and XOR operation is performed between values of the b_0, b_4, b_5, b_7, b_{10}, b_{12}, b_{14}, and b_{15} bits.

The result of XOR is given as feedback. The resultant binary sequence is converted into decimal and stored in $K3$.

Step 8. Again, Step 7 is repeated by considering binary value of $K3$ as seed value to generate another sequence and stored in $K4$.

Step 9. Then, values of $K2$, $K3$, and $K4$ are XORed to produce SK.

$$\mathrm{SK} = K2\,(\mathrm{XOR})\,K3\,(\mathrm{XOR})\,K4. \tag{2}$$

Step 10. MHN node sends a key SK generated in Step 8 to the sender node by encrypting it with public key of sender node.

$$E_{SPUB}\,(\mathrm{SK}). \tag{3}$$

S_{PUB} represents the sender node's public key.

Step 11. After receiving encrypted SK from MHN node, the sender node performs decryption by using its private key to obtain SK. After obtaining SK, the sender node performs two-level encryption as follows.

$C1 = M^e \bmod n$//encryption by using sender node's public key generated by RSA algorithm.

$C1$ represents the ciphertext produced after performing encryption. The ciphertext obtained is then XORed with SK to produce final ciphertext that is sent to the receiver.

$$C = C1\,(\mathrm{XOR})\,\mathrm{SK} \tag{4}$$

is the final ciphertext which is transmitted to the receiver node.

3.1.2. Decryption Process

Step 1. RSA algorithm is used to generate public and private keys at receiver node.

Step 2. After receiving encrypted message, receiver node requests SK from MHN node by sending KREQ packet.

Step 3. MHN node sends SK by encrypting it with the public key of receiver node.

$$E_{RPUB}\,(\mathrm{SK}). \tag{5}$$

R_{PUB} represents the receiver node's public key.

Step 4. After receiving encrypted SK from MHN, the receiver node performs decryption by using its private key to obtain SK. After retrieving SK, the receiver node performs the decryption of ciphertext as follows.

$$C1 = C\,(\mathrm{XOR})\,\mathrm{SK}. \tag{6}$$

Received ciphertext is XORed with SK to obtain $C1$. $C1$ is decrypted using receiver node's private key to obtain the plaintext M.

$M = (C1)^d \bmod n$//decryption by using receiver node's private key generated by RSA algorithm.

By using a logistic map-based key generation technique, encryption and decryption operations are performed in MANET for secure information exchange. The usage of the logistic map function improves and strengthens the encryption algorithm. Also, this approach is suitable for MANET because the proposed approach provides high security and low cost of implementation. We have performed two-level encryption such that guessing of key and prediction of plaintext becomes difficult for an attacker. Moreover, all the activities of nodes are also monitored by the MHN node. We also designed our proposed model in such a way that if any malicious node that continuously generates KREQ packets with an intention to launch a DoS attack then such nodes will be identified by the MHN node. If any node continuously sends 3 KREQ packets, then MHN will mark that node as malicious node and such node will be detached from the network. This proposed security model is less expensive than the existing approaches that involve Trusted Third Party or Certificate Authority for issuing of public certificates [22–27]. The proposed approach objectives can extend using other extensive technologies as a part of Industry 5.0 [2, 11–15, 28–31].

4. Performance Evaluation

We evaluated the performance of the proposed security model through simulation in NS2. We evaluated the performance of our proposed approach by launching DoS and blackhole attacks in NS2. Figure 4 depicts the communication among healthcare nodes and MHN. Table 2 shows the simulation parameters considered in NS2 for evaluating the proposed methodology. We analyzed the performance of the proposed methodology by simulation in NS2. We tested the proposed method by varying number of nodes, i.e., 50, 100, and 150 nodes.

4.1. Key Generation Time. Figure 5 justifies that the proposed hybrid logistic map-based cryptographic algorithm exhibits less key generation time than the existing approaches. The key generation time includes private key, public key, and session key generation time. Also, key generation time is measured by considering different key lengths.

4.2. Encryption Time. Encryption time is a time taken to obtain ciphertext from the given plain text. It specifies the speed of encryption algorithm. Table 3 represents the efficiency of the proposed cryptosystem in terms of encryption time with respect to the varying packet sizes. The proposed approach is compared with RSA-3DES and RSA-AES techniques because in the proposed methodology we used

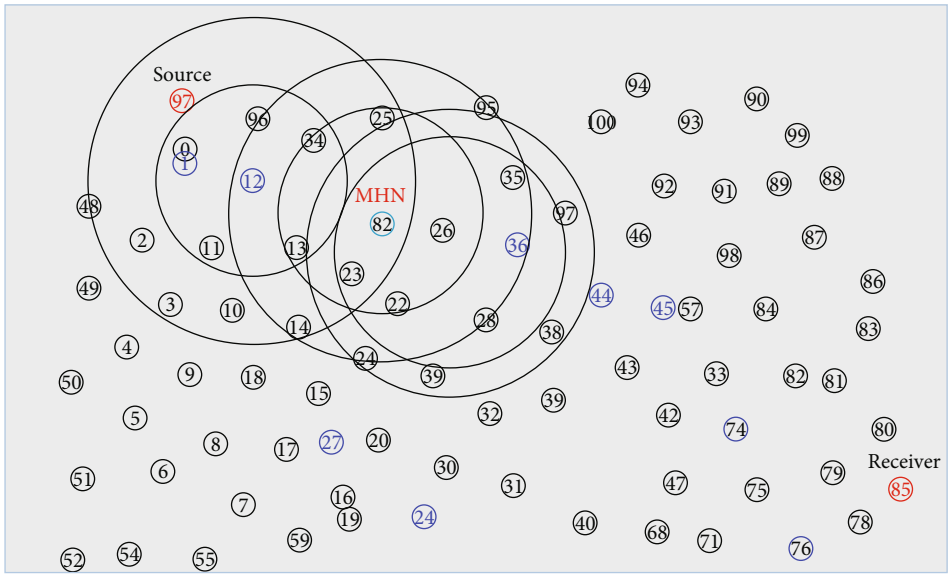

Figure 4: Healthcare network formulation in NS2 using the proposed network model.

Table 2: Simulation parameters.

Parameters	Values
Coverage area	500 m × 500 m
Simulation time	500 sec
No. of nodes	50, 150, and 200
Traffic type	UDP-CBR
Transmission range	250 m
Packet size	512 bytes
Maximum speed	20 m/s
Routing protocol	I-AODV [6] [7]
Mobility model	Random way point

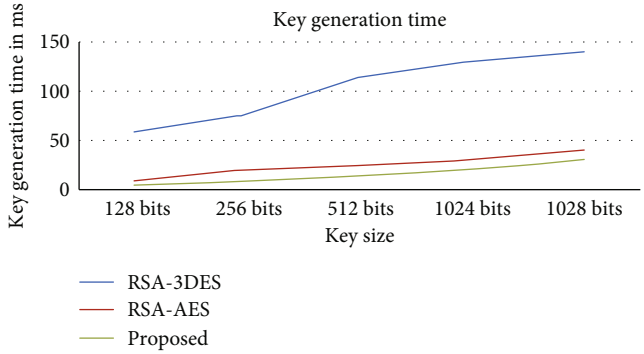

Figure 5: Key generation time of the proposed cryptosystem.

RSA-based approach for generation of public key and private key. Figure 6 justifies that the proposed cryptosystem requires less encryption time when compared with the existing hybrid cryptographic schemes.

4.3. PDR under Presence of DoS Attack. Packet delivery ratio (PDR) is the ratio of total number of packets

Table 3: Comparison of encryption time.

Packet size	RSA-3DES	RSA-AES	Proposed
512 bytes	165.45 ms	185.6 ms	110.8 ms
1 KB	302.45 ms	321.45 ms	199.78 ms
5 KB	467.86 ms	623.57 ms	319.2 ms
10 KB	654.54 ms	805.94 ms	578.32 ms

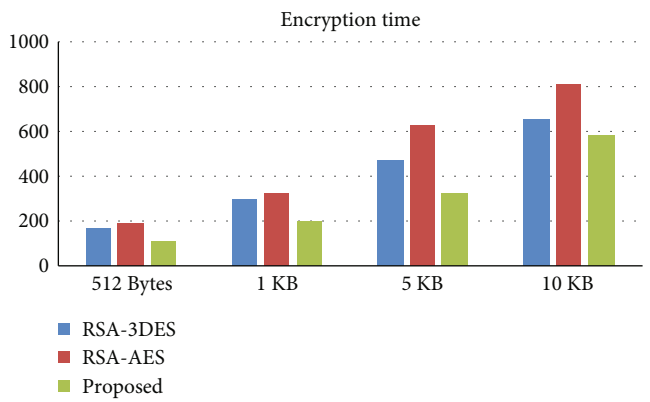

Figure 6: Comparison of encryption time.

received at destination and the total number of packets sent by the sender.

$$\text{PDR} = \frac{\text{total number of packets received at destination}}{\text{total numbr of packets sent by the sender}} * 100. \quad (7)$$

Our simulation result justifies that the proposed hybrid cryptographic scheme gives better PDR than the existing protocols even in the case of DoS attacks. Figure 7 demonstrates that the proposed scheme exhibits better PDR ratio even in the case of increasing number of nodes.

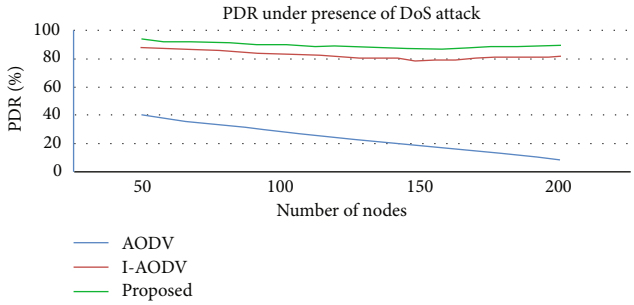

Figure 7: Comparison of PDR in the presence of DoS attack.

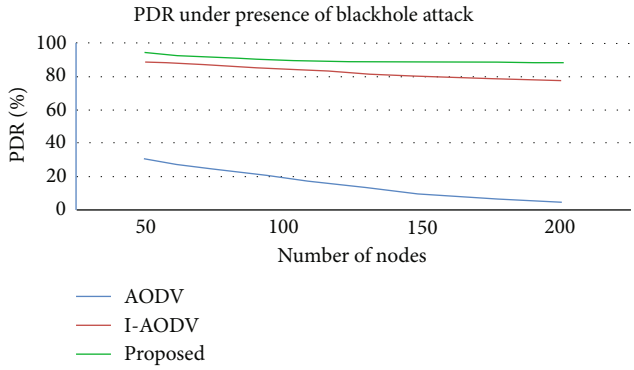

Figure 8: Comparison of PDR in the presence of blackhole attack.

4.4. PDR under Presence of Blackhole Attack. Figure 8 demonstrates that the proposed methodology exhibits 94% PDR than the existing protocols in the presence of blackhole attack.

5. Conclusion and Future Work

In this paper, we proposed a hybrid logistic map-based cryptographic approach for MANET-based healthcare system for secure medical information exchange. Our simulation results showcase the efficiency of the proposed cryptosystem in terms of key generation time, encryption time, and better PDR even in the presence of DoS and blackhole attacks. The proposed MANET-based healthcare network can handle DoS and blackhole attacks efficiently. The proposed cryptosystem is also compatible with all the cluster-based routing approaches designed for MANET-based applications. The proposed network model is energy efficient and allows mobile healthcare nodes to exchange information securely. Furthermore, our proposed system relinquishes the CA or TTP that performs key management activities in existing approaches. In the future, we modify this proposed methodology to handle other attacks like grayhole attack and jellyfish attack in MANET-based healthcare systems to ensure better security with minimum overhead.

Data Availability

The data used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Rama Krishna and M. Sirajuddin, "A role of emerging technologies in the design of novel framework for COVID-19 data analysis and decision support system," *Computational Intelligence*, vol. 963, pp. 313–337, 2022.

[2] W. Wang, C. Qiu, Z. Yin et al., "Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2021.

[3] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, vol. 14, 2021.

[4] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: a trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network," *Security and Communication Networks*, Article ID 5521713, 9 pages, 2021.

[5] A. Ahmad and S. Ismail, "User selective encryption method for securing MANET," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3103–3111, 2018.

[6] A. Echchaachoui, A. Choukri, A. Habbani, and M. Elkoutbi, "Asymmetric and dynamic encryption for routing security in MANETs," in *2014 International Conference on Multimedia Computing and Systems (ICMCS)*, pp. 825–830, Morocco, April 2014.

[7] A. Khan, Q. T. Sun, Z. Mahmood, and A. U. Ghafoor, "Energy efficient partial permutation encryption on network coded MANETs," *Journal of Electrical and Computer Engineering*, vol. 2017, 10 pages, 2017.

[8] R. A. Hamamreh, M. Ayyad, and M. Jamoos, "RAD: reinforcement authentication DYMO protocol for MANET," in *2019 International Conference on Promising Electronic Technologies (ICPET)*, pp. 136–141, Gaza, October 2019.

[9] 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 (IJARET)*, vol. 11, no. 3, pp. 91–107, 2020.

[10] H. Xiong, "On the design of blockchain-based ECDSA with fault-tolerant batch verication protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, 2021.

[11] C. Rupa and D. J. Kumari, "Network-based adaptation of blockchain technology," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9, pp. 141–148, 2019.

[12] V. Nikhila and C. Rupa, "Intensifying multimedia information security using comprehensive cipher," in *2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, pp. 1–4, Vellore, March 2019.

[13] S. Gadamsetty, R. Ch, A. Ch, C. Iwendi, and T. R. Gadekallu, "Hash-based deep learning approach for remote sensing satellite imagery detection," *Water*, vol. 14, no. 5, article 707, 2022.

[14] S. Juneja, G. Dhiman, S. Kautish, W. Viriyasitavat, and K. Yadav, "A perspective roadmap for IoMT-based early detection and care of the neural disorder, dementia," *Journal*

of Healthcare Engineering, vol. 2021, Article ID 6712424, 11 pages, 2021.

[15] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, "A metaheuristic optimization approach for energy efficiency in the IoT networks," *Software: Practice and Experience*, vol. 51, no. 12, pp. 2558–2571, 2021.

[16] A. Sharma, "Localization in wireless sensor networks for accurate event detection," *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 16, no. 3, pp. 74–88, 2021.

[17] C. U. Bhaskar and C. Rupa, "An advanced symmetric block cipher based on chaotic systems," in *2017 Innovations in Power and Advanced Computing Technologies (i-PACT*, pp. 1–4, Vellore, April 2017.

[18] C. Mohammad Sirajuddin and R. A. Prasad, "A novel key management technique for secure data communication by reducing packet dropping and energy consumption in MANET," *Ciencia e Tecnica Vitivinicola*, vol. 34, pp. 2416–3953, 2019.

[19] M. Sirajuddin, C. Rupa, and A. Prasad, "A trusted model using improved-AODV in MANETS with packet loss reduction mechanism," *Advances in Modelling and Analysis B*, vol. 61, no. 1, pp. 15–22.

[20] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar, P. K. Singh, and W.-C. Hong, "An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare," *Sensors*, vol. 20, no. 14, p. 3887, 2020.

[21] D. K. Bangotra, Y. Singh, N. Kumar, P. Kumar Singh, and A. Ojeniyi, "Energy-efficient and secure opportunistic routing protocol for WSN: performance analysis with nature-inspired algorithms and its application in biomedical applications," *BioMed Research International*, vol. 2022, Article ID 1976694, 13 pages, 2022.

[22] G. Santhanamari, J. Premi, S. Rahavi, and S. Vijay, "Health monitoring of soldiers using efficient Manet protocol," in *2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, pp. 57–62, Kerala, December 2020.

[23] R. Mahajan and S. Zafar, "DDoS attacks impact on data transfer in IOT-MANET-based E-healthcare for tackling COVID-19," in *Data Analytics and Management*pp. 301–309, Springer, Singapore.

[24] K. Saravanan and J. Vellingiri, "Defending MANET against flooding attack for medical application," in *2017 2nd International Conference on Communication and Electronics Systems*, pp. 486–489, Coimbatore, October 2017.

[25] N. Veeraiah, O. Ibrahim Khalaf, C. V. P. R. Prasad et al., "Trust aware secure energy efficient hybrid protocol for MANET," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.

[26] N. N. Malik, M. Irfan Alosaimi, and B. Uddin, "Wireless sensor network applications in healthcare and precision agriculture," *Engineering*, vol. 2020, article 8836613, pp. 1–9, 2020.

[27] P. Sathyaraj and D. Rukmani Devi, "Retracted article: Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method," *Computing*, vol. 12, no. 7, pp. 6987–6995, 2021.

[28] C. Iwendi, Z. Jalil, A. R. Javed et al., "KeySplitWatermark: zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[29] M. Khamruddin and C. Rupa, "A rule based DDoS detection and mitigation technique," in *2012 Nirma University International Conference on Engineering*, pp. 1–5, Ahmedabad, India, 2012.

[30] C. Rupa and D. Midhunchakkaravarthy, "Preserve security to medical evidences using blockchain technology," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 438–443, Madurai, India, May 2020.

[31] K. L. S. Priya and C. Rupa, "Block chain technology based electoral franchise," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pp. 1–5, Bangalore, March 2020.