

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications



ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks

B. V. V. Siva Prasad, Sridhar Mandapati, Lakshmana Kumar Ramasamy, Rajasekhar Boddu, Pranayanath Reddy & B. Suresh Kumar

To cite this article: B. V. V. Siva Prasad, Sridhar Mandapati, Lakshmana Kumar Ramasamy, Rajasekhar Boddu, Pranayanath Reddy & B. Suresh Kumar (2023) Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks, *Automatika*, 64:3, 658-671, DOI: [10.1080/00051144.2023.2203564](https://doi.org/10.1080/00051144.2023.2203564)

To link to this article: <https://doi.org/10.1080/00051144.2023.2203564>



© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 04 May 2023.



Submit your article to this journal [↗](#)



Article views: 1019









View related articles [↗](#)



View Crossmark data [↗](#)



Ensemble-based cryptography for soldiers' health monitoring using mobile ad hoc networks

B. V. V. Siva Prasad ^a, Sridhar Mandapati ^b, Lakshmana Kumar Ramasamy ^c, Rajasekhar Boddu ^d,
Pranayanath Reddy ^e and B. Suresh Kumar ^f

^aAnurag University, Telangana, India; ^bDepartment of Computer Applications, R. V. R & J. C College of Engineering, Guntur, India; ^cFaculty of Computer Information Science, Higher Colleges of Technology, Ras Al- Khaimah, United Arab Emirates; ^dDepartment of Software Engineering, College of Computing and Informatics, Haramaya University, Dire Dawa, Ethiopia; ^eDepartment of CSE, GITAM School of Technology, GITAM (Deemed to be University), Hyderabad, India; ^fDean School of Computer Science and Engineering, Sanjay Ghodawat University, Kolhapur, India

ABSTRACT

Information technology acts an important role in gathering, transmitting with executing data from areas of disaster-prone such as the battlefield and international borders. In addition to the country's security, the soldier needs protection by defending himself with advanced weapons such as a bomb detector. This paper provides the capability to track the whereabouts and health of soldiers who have been lost or injured on the battlefield. It assists in reducing the time, searching and rescuing operation efforts of the military control room. This paper implements a system for health-condition monitoring that sends soldiers' health parameters, such as the electrocardiogram (ECG), blood oxygen level, pulse rate, and temperature, to the control room via a Mobile Ad hoc Network (MANET). Body parameters are sensed utilizing various body sensors fixed to the bodies of soldiers. The body parameters are broadcasted to the control room via MANET devices at the path. To preserve the health parameters data of soldiers from enemies while data transmission, this paper also proposes a cryptographic ensemble approach. This approach combines Symmetric Key Encryption, and Identity Based Encryption (IBE) with Identity Based Signature (IBS). The experimental result shows proposed cryptographic ensemble provides high security compared with existing MANET security algorithms.

ARTICLE HISTORY

Received 2 September 2022
Accepted 12 April 2023

KEYWORDS

Cryptography; data transmission; health monitoring; MANET; routing

1. Introduction

Soldiers should be monitored by sophisticated health-care, actual-time Global Positioning System with information exchanges to transmit and obtain data from/to the control room [1]. For that soldiers may require MANET not merely to the contact control room alongside army staff. Despite the country's protection, soldiers should require security by defending them with sophisticated weapons. In addition, the military control room needs to supervise the health condition of the soldier. Bio-medical sensors with monitoring devices are incorporated by the soldiers. The included elements should be lightweight with the presently preferred outcome with no need for more energy. One of the primary challenges at armed functions lies that the soldiers cannot contact the control room.

Additionally, the correct routing among soldiers acts as a significant task for cautious preparation with synchronization. Thus, this paper focuses on tracking the place of the soldier which is helpful for the control room to identify his precise position and direct him. The

control room tracks the position of the soldier using GPS. The control room needs to lead the soldier on the right pathway if he is missing in the war field. This paper would be helpful for soldiers who engage in special missions or assignments. Intelligent Bio-medical sensors incorporating bomb detectors, vibration sensors, humidity and temperature sensors, ECG modules, Heartbeat sensors and so on are affixed to the jacket of soldiers [2]. The soldier fixes these for full mobility. This scheme would offer a link to the control room utilising MANET. The information gathered in the control room could be used for further investigation. It might assist the control room to recognize the circumstances in the war field [3–5].

MANET networks are huge with difficulty, mainly in battery life and energy competence [6,7]. The existing routing protocols for MANET are hard and also need enormous memory with processing power that are inadequate assets for the devices, including a MANET network [8,9]. Thus, there is a requirement for a simpler routing algorithm that is capable of efficaciously

preserving the power of the devices [10]. To deal with this issue, this paper proposes the Minimum Energy Expenditure Routing (MEER) algorithm. It decreases power expenditure proficiently.

To protect the health parameter information of soldiers from enemies during data transmission cryptography technique is needed. The use of codes to secure information and communications in such a way that only the intended recipients can decipher and process them is known as cryptography. Hence, information access by unauthorized parties is prevented. In the age of computers, cryptography is frequently associated with the conversion of plain text into ciphertext, which is the text that can only be decoded by the intended recipient. This process is known as encryption. Decryption is the process of converting encrypted text into plain text.

There are generally three different forms of cryptography:

Symmetric key cryptography: It is an encryption technique where messages are encrypted and decrypted using the same shared key by both the sender and the recipient. Symmetric Key Systems are quicker and easier, but the issue is that the sender and receiver must securely exchange keys. The Data Encryption System (DES) is the most widely used symmetric key encryption system.

Hash functions: This algorithm uses no keys at all. It is impossible to reconstruct the contents of plain text since a fixed-length hash value is computed based on plain text. Hash functions are widely used in operating systems to secure passwords.

Asymmetric key cryptography: In this approach, information is encrypted and decrypted using a pair of keys. When encrypting data, a public key is utilized, and when decrypting data, a private key is utilized. Private Key and Public Key are distinct. Even if everyone knows the public key, only the intended recipient can decode the message because only he has access to the private key.

This paper further proposes a cryptographic ensemble approach to protect the health parameter information of soldiers from enemies during data transmission. This approach combines Symmetric Key Encryption, Identity-Based Encryption (IBE) with Identity-Based Signature (IBS).

The rest of the paper is organized as follows. Section 2 discusses associated work dealing with the existing routing algorithms and cryptography techniques for MANET devices. Furthermore, Section 3 explains the preliminaries of the MEER routing and the cryptographic ensemble approach. Section 4 explains the methodology of the proposed work with the experimental results explained in Section 5. Lastly, the lessons learned with conclusions are summarized in Section 6.

2. Related works

This section presents the related work of the existing routing algorithms and cryptography techniques for MANET.

Chen et al. [11] presented a routing protocol, namely topological change Adaptive Ad hoc On-demand Multipath Distance Vector (TA-AOMDV) that could adapt to rapid device progress to sustain QoS. A constant route choice algorithm is developed in this protocol, which not merely gets node resources (queue length, available bandwidth and residual energy) like the route choice parameters. However, it further regards the connection constancy probability among nodes. In addition, to adapt to the quick transformation of the topology, the connection disrupts the forecast method that is incorporated into the protocol, which modernises the routing plan using episodic probabilistic estimation of connection steadiness.

Khudayer et al. [12]'s aim to get better on-demand source routing protocols by suggesting a link failure prediction mechanism (LFPM) and a zone-based route discovery mechanism (ZRDM). ZRDM's objective is to manage the flood of path requests with LFPM goals to avoid route disruptions due to the node movement. The performance of the methods was assessed using NS3 using average end-to-end delay, packet delivery ratio and regularized routing load.

Li et al. [13] provided a method, namely DAPV, which could discover solitary or joint malicious devices and also the paralyzed devices which act unusually. DAPV could discover both indirect and direct attacks initiated during the routing stage. To discover abnormal or malicious devices, DAPV depends on two major methods. Initially, the origin tracking allows the hosts to infer anticipated log data of the peers by the identified log entry. Next, confidentiality-protecting confirmation uses the Merkle Hash Tree to check the logs devoid of enlightening any device's confidentiality. The authors show the efficiency of their method by relating DAPV to three situations: (1) discovering inserted malevolent middle routers that assign passive and active attacks at MANET; (2) opposing the joint blackhole attack of the AODV protocol, also; (3) discovering paralyzed routers at the university campus network.

Zhang et al. [14] determined the problem of data deliverance at MANET goal to enhance the quality of service (QoS) and the quality of experience (QoE) users receive. MANETs have recurrent disconnections with huge rates of failed broadcasts as MSDs shift in and out of network coverage fields. Also, the topology continually alters. To resolve these problems, the major offerings of this work are as follows: (1) the authors examined the QoE-driven multipath TCP (MPTCP)-based information deliverance form at MANET; (2) the authors provided hidden Markov model-based

best-start multipath routing, which could efficiently forecast mobile devices close to future network link condition along with its precedent link condition; (3) the authors leveraged MPTCP to concurrently broadcast information by numerous interfaces of MSDs also enhance the organization technique for MPTCP sub-paths; also (4) the authors learned and enhanced the algorithm of multihop routing in MANETs.

Khan et al. [15] presented a Certificateless Key-Encapsulated Signcryption (CL-KESC) system. The system is using the idea of Certificateless Public Key Cryptography (CL-PKC). As CL-PKC is protected from key escrow issues, the main disadvantages of Identity-based Public Key Cryptography (ID-PKC) are tackled. Alas, the previous creation methods of CL-KESC depend on elliptic curve-based functions, which are computationally luxurious for small UAVs. The authors provided a novel creation method of CL-KESC using Hyperelliptic Curve Cryptography (HECC) to solve the problem.

Elhoseny and Shankar [16] focused on enhancing reliable information broadcast by huge safety at the MANET using an optimization method. At the MANET, the devices are grouped using a power-efficient routing protocol. After that, the customized separate particle swarm optimization is used to choose the best cluster head. A secure routing and a signcryption method could be utilized to enhance a broadcast safety of a dependable MANET. The signcryption algorithm encrypts the digital signature that could improve the whole competence with privacy.

Farouk et al. [17] presented confidentiality protecting Fully Homomorphic Encryption over the Advanced Encryption Standard (P 2 FHE-AES) system for the LBS question. It is necessary for position confidentiality security to support drivers to use this service with no danger of being followed. It is enhanced by utilizing Cloud simulation (CloudSim) and Simulation of Urban Mobility (SUMO) with NS-2.

Anbarasan et al. [18] focused on the safety of the hoped MANETs. It presents robust and rigid networks, while supplementary assets are attached. For grouping the devices, the LEACH protocol is recommended for the CMs and CHs are fixed for the information transmit at the network. The power is dispersed at the LEACH to evade the network's fatal and battery exhaust. Therefore, to add confrontation and create an authentic network, the encoding and decryption are integrated as an addition to evade the DoS attacks.

Shukla et al. [19] presented a protocol to alleviate the black hole attack with a wormhole attack. The protocol is a mixture of measurable-energetic elliptic curve cryptography also AODV protocol, namely ECCAODV. The authors have regarded the 2D vector function $F[A, B]$. Here A is a Wormhole Attack and B is a Blackhole attack. For checking their presented

protocol, the authors have regarded situations primarily with no attack and with the attack. While there is no attack, the authors have symbolized that as AODV at graphs also the attack, the authors have explained it like MAODV.

Elmahdi et al. [20] presented dependable and safe information broadcast at MANET's beneath feasible blackhole attacks using altered ad-hoc on-demand multipath distance vector (AOMDV) protocol. They separated the data into numerous routes to the target and also used the homomorphic encryption system for the cryptography method. The system's effectiveness is constant by an extremely huge packet delivery ratio as that of AOMDV is established to be susceptible to the interruption of malevolent devices at the MANET.

Muruganandam et al. [21] provided a proficient Real-time Reliable Clustering and Secure Transmission (RRCST) technique. The method creates by clustering the devices at an area where the choice of cluster head is executed along with the preceding broadcast performance device data. The devices are grouped using their aspects of geography. Also, the cluster head is selected from every cluster using a variety of sustain procedures calculated overpower, broadcast and geographic characteristics. Additionally, the routing is executed using a new technique that chooses the path using the value of reliable transmission support (RTS) computed for various paths. Furthermore, the technique chooses a path using a variety of QoS sustain values calculated for every path.

Khanna et al. [22] provided a broad taxonomy of the alleviation and discovery method and summarization and contrast of a few available works associated with those groups. There are a whole 16 various groups of alleviation methods. They have also appraised ninety-one investigated workings associated with the provided group on a variety of parameters similar to overhead, alteration at the base routing protocol, discovery type and characteristics with boundaries.

Thiagarajan et al. [23] presented a framework that assists in discovering the malicious devices in each destination. After the discovery procedure, it is isolated and surplus while routing the organization by various methods. The development of an algorithm that supports dependable Multipath Routing which assists in determining routes for a collection of disjoint devices. Using the index of dependability, the paths are rearranged. At present, the procedure of data in the form of information is detached from source to destination. The major route is a group to transmit the data. The last goal in the case of disparity of data sent from a source while received at the destination then there is a criticism that there is a disparity of information with the data associated with the broadcast and also its route. Thus, the destination would be capable of getting better as the data are verified every time for dependability.

Abebe et al. [24] presented proficient FPGA-based incorporated cryptosystems for the safety of the high-presentation stage, controlled devices and safe data swap, focusing on the protection of healthcare IoT to tackle the challenges. Fewer algorithms are used to attain superior throughput and lesser region appropriate for the exact executions when saving more space, key management and key storage necessities than previous report results.

Mahamune et al. [25] provided a comprehensive review of TCP or IP layer-wise MANET attacks with equivalent protection methods. A MANET situation using Ad Hoc On-demand Distance Vector (AODV) is surrounded also experienced beneath the routing disruption attacks viz. grey hole, black hole and also a cooperative black hole. The attacks are simulated at the EXata surroundings to decide their occurrence over others in changeable network situations. The relative presentation study is further carried out using the capacity of the high-tech assessment metrics similar to jitter, throughput and end-to-end delay. Also, the amount of information data were dropped through malicious devices.

Suma et al. [26] regarded the safety problems concerning a secured identity-based location-aware routing (SIBLAR) with location-aided routing (LAR) protocol to attain the system's safety by an enhanced key refreshment method. MANET situations were produced at ns2 also the competence of the SIBLAR was estimated using specific performance metrics. During safety attacks, the SIBLAR system is established as proficient compared to essential LAR.

Medeiros et al. [27] presented a new ILP multi-objective method, known as Multi-objective routing Aware of miXed traffic (MAXI). It uses three weighted goals to lead the routing at WMNs by various appliances with necessities. Additionally, it presents comparative research by other related attitudes of routing using NS-3 to assess using simulation, which gets into account various kinds and stages of interruption (for instance, co-channel interruption with outside interruption) concentrated on assorted IoT traffic for aged healthcare vision. Finally, it demonstrates the effectiveness of the proposed method to accommodate the needs of each device through appropriate objective functions. The routes with the shortest paths are chosen while using the Joint technique for Improving Load Balance and Path Length (JILP) for a bi-objective optimization of WMN. The Joint Routing, Channel Assignment and Rate Allocation Heuristic (JRCAR) chooses the routing for the flows to lessen the overload links, while also attempting to choose shorter paths to shorten the path length of each flow.

IoT cuts through any field that require contact or supervision. The current mechanisms of the IoT focus on structural design, secure contact, topography, sites and so on. In the health sector, actual-time right of

entry is to sensor information such as GSR sensor, EEG sensor, EMG sensor, glucometer, ECG sensor, weight measurement, BP sensor and Pulse SpO2 sensor. Many of the current mechanisms concentrate on the strength of encryption with authentication methods. Less attention is paid to the need for a lightweight security plan for the actual-time right of entry to small executing devices. Quist-Aphetsi and Xenya [28] bridge the gaps using Diffie-Hellman key distribution for medical device authentication with the DES for the encryption of health-associated information transmission.

Encryption is an important problem for keeping the confidentiality of information in healthcare appliances. A proficient method of encryption with less energy expenditure is preferred for the IoT. Khader et al. [29] proposed power-efficient encryption by adapting the AES algorithm to suit the IoT sensors. The modernized algorithm assessed that the time of the session is compared with the time of brute force.

A safety-based system with less energy expenditure for small devices has been proposed by Kondawar et al. [30]. Their system gathers data from the patient's physical parameters, executes the data, encrypts and broadcasts the data wirelessly. It further contains encryption and, lastly, data display on the system. Encryption is completed by enabling the encryption algorithm, for example, Blowfish on the ARM7 controller. Decryption is completed on the system on the side of doctors. Information from the sensors was safely transmitted to the recipient with less energy expenditure. More patients will benefit as this system is available at a lower cost.

The first ID-based Fully Homomorphic Encryption (IBFHE) programme was built from lattice-based cryptography with Identity-Based Encryption (IBE) by Waters, Sahai with Gentry at CRYPTO 2013. Their IBFHE program was enhanced by Shen et al. [31], using Peikert's tight and Alborin-Sheriff and easy noise research methods to evaluate homomorphic and Peikert's with Micciancio strong and a new trapdoor. Utilizing a mask program, the authors create a fully homomorphic encryption (MIFHE) program that can increase a "new" cypher text beneath a solitary identity key to an "extended" one beneath a merged key which permits cypher texts underneath various ids to be homomorphically assessed.

For wireless sensor networks, Rango et al. [32] introduced a unique distributed shortest hop multipath method (SHM) to produce energy-efficient pathways for data routing or dissemination. Rango et al. [32] proposed the Multipath Energy Aware DSR (MEA-DSR). The MEA-DSR is an addition to the DSR (Dynamic Source Routing protocol) protocol that calculates various node-disjoint pathways, with the "optimal" path being the most energy-efficient.

To study the MANET multipath routing problem, Sun et al. [33] discussed the multipath routing problem,

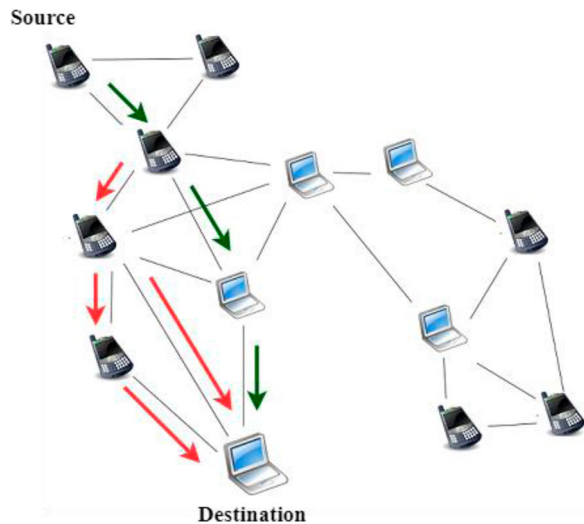


Figure 1. MANET routing.

which might be related to the energy entropy model. In MANET, they presented an Energy Entropy-based minimum Power cost Multipath routing algorithm (EEPMM). To provide load balancing in the MANET whose topology changes continuously, the main idea behind the EEPMM method is to generate a new metric entropy and select the stability multipath with the aid of that metric.

The next section outlines the fundamentals of MANET routing and cryptography, in particular encryption and decryption with the creation of digital signatures.

3. Preliminaries

This section provides the preliminaries of the proposed cryptographic ensemble approach for Privacy-Preserving Health Monitoring of Soldiers Using MANET. It mainly discussed routing and cryptography in MANET.

3.1. Routing

Routing is the procedure of choosing a route across one or more systems [37]. Figure 1 shows the routing procedure of MANET. In Figure 1, a source device finds the shortest path to a destination device.

Routers denote inner routing tables to create choices regarding how to path data next to network routes. The routing table stores the routes that data must attain to each destination that the router is accountable. Routing tables are similar to that, however, for network routes instead of trains. Think about train schedules, which train travellers ask to determine which train to catch.

Routers job at the subsequent method: If a router obtains data, it studies the data headers to view its planned target. It decides where to path the data using

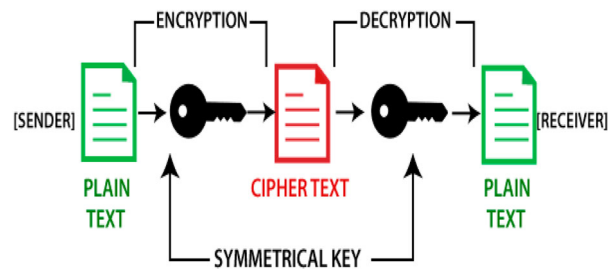


Figure 2. Encryption and decryption.

the data at its routing table. A train conductor can verify the tickets of the passengers to decide which train to take.

Routers perform these millions of times a second with millions of data. As data move towards their target, it can be diverted more times by various routers. In MANET, every mobile device performs as a Router.

3.2. Cryptography

Cryptography is the study of safe interaction methods that permit merely the sender of a message and the desired recipient to see its contents [38]. Data could be encrypted to create it hard to steal the information. A lot of words are used in cryptography, and a few are explained below.

3.2.1. Encryption and decryption

Figure 2 shows the process of encryption and decryption. Encryption is the technique of changing information into random alphabets and numbers, which creates it meaningless but not for the planned receiver. It is the procedure of encrypting plaintext to ciphertext. During the encryption procedure, the data are referred to as plaintext, while the converted data are referred to as ciphertext.

Decryption could be explained as the procedure of converting back the encrypted content into real data. It is the overturned procedure of encryption. A planned receiver could merely decrypt the content by using the secret key.

3.2.2. Digital signature generation

A digital signature is a mathematical method used to generate digital codes used to set up the legitimacy of digital messages and documents. These codes are produced and validated through the HmacSHA1 algorithm. The data also the sender's specifications are checked by affixing the signature to the automatically dispersed document.

The methodology for Soldiers Health Monitoring Using Mobile Ad hoc Networks is discussed in the following section, with a focus on the Minimum Energy Expenditure Routing (MEER) algorithm and a cryptographic ensemble approach.

4. Methodology

This section tracks the location and health of lost or wounded soldiers on the battlefield. It helps to reduce the time, search and retrieve operational efforts of the military control room. This section implements a system for health-condition monitoring that sends soldiers' health parameters such as ECG, blood oxygen level, pulse rate and temperature to the control room via MANET. Body parameters are sensed using various sensors fixed to the soldier's body. Body parameters are broadcasted to the control room via MANET devices along the path (for example, devices of the soldiers act as MANET devices to transmit data). The body parameters collected in the control room can be used for further data analysis. Most devices on the MANET run on battery. These battery-powered terminals remain lively for a long time devoid of any personal manages after early exploitation. A MANET device will discharge its battery within a few days because of the lack of power-efficient methods. Even in communications, a lot of energy is wasted in states such as conflict, control packet overhead and interruption. Therefore, many routing protocols have already been designed to reduce power consumption and improve network life. Conventional reactive routing algorithms such as Dynamic Source Routing (DSR) and ad hoc on-demand distance vector (AODV) are implemented to detect the shortest route devoid of considering the power expenditure of a MANET device. So the particular exact device could be chosen frequently, which can shorten the device's life span.

Conversely, the present routing algorithms use the hop number like their path choice metric to discover the shortest route among the sources with target devices. But, since the routing metric is incompatible with the dynamic network topology on the MANET, it is only appropriate to use the hop number because it does not feel for packet loss, data rates, connection capacity, connection quality, interference or many other routing requirements. Furthermore, these routing protocols cannot effectively reduce the power consumption of MANET devices. This chapter proposed the Minimum Energy Expenditure Routing (MEER) algorithm for MANET to deal with these problems. Figure 3 shows the architecture of Health Monitoring of Soldiers using MANET. In Figure 3, a source device fixed in a soldier collect the health parameters of that soldier and finds the shortest path to a control room. Then these health parameters are forwarded to the control room via this discovered shortest route.

4.1. Minimum energy expenditure routing

The Proposed Minimum Energy Expenditure Routing algorithm is classified into two sub-algorithms: Compute Direction and Distance algorithm and Estimate Energy Expenditure algorithm.

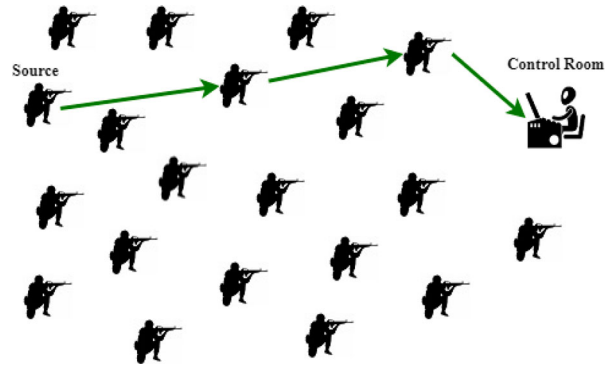


Figure 3. Health monitoring of soldiers using MANET.

Algorithm 1: The Minimum Energy Expenditure Routing (MEER) Algorithm

```

Input   : Control Room (CR), MANET Devices (MDs), All MANET Devices
          Location List (LI)
Output  : Minimum Energy Expenditure Route (MEER)
Step 1  : MANET_Network_Formation (CR, MDs, LI)
Step 2  : Sleep_Scheduling (MDs)
Step 3  : DirectDist[] = Compute_Direction_Distance (MDs,CR,LI) //
          Algorithm 2
Step 4  : SortedDirectDist[] = Sort all MDs Devices Based on Direction
          and Distance
Step 5  : SDD[] = Sort once again, including Single Direction
Step 6  : For each Src from MDs
Step 7  : Routes[] = Extract all available Routes for Src from SDD
Step 8  : IE = Estimate_Energy_Expenditure(R0) // R0 - First Route
Step 9  : ME = IE, MEER = R0 // ME - Minimum Energy
Step 10 : For each Route Ri in Routes do // Ri Starts from the Second
          Route
Step 11 :     Energy = Estimate_Energy_Expenditure(Ri) //
          Algorithm 3
Step 12 :     If (Energy < ME)
Step 13 :         ME = Energy
Step 14 :         MEER = Ri
Step 15 :     End If
Step 16 : End For
Step 17 : Wake_Up_and_Inform_about_MEER (Src)
Step 18 : Sleep_Scheduling (Src)
Step 19 : End For

```

Algorithm 1 discusses the MEER routing. It originally builds the MANET using the location list of the control room with MANET devices. Also, it puts all MANET devices to sleep. And it uses two sub-algorithms.

The first sub-algorithm calculates all MANET Devices, Direction and Distance values from the MANET Control Room using its geo-location values (the x -axis (Latitude), the y -axis (Longitude)) with Euclidean Distance.

$$DT = \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)} \quad (1)$$

The control room will find all available paths for each MANET device based on the direction and distance values. Algorithm 2 discusses the Direction and Distance Computation algorithm.

Algorithm 3 discusses Energy Expenditure Estimation. After that, it estimates energy costs in all available

Algorithm 2: Compute_Direction_Distance (Compute Each MANET Device's Direction and Distance from the Control Room)

Input : MANET Devices (MDs), Control Room (CR), All MANET Devices with CR Location List (LI)
Output : Each MANET Device's direction and distance details from the Control Room (DirectDist)

Step 1 : DirectDist[] = , i = 0
Step 2 : Loc1 = Extract the Location of CR from LI
Step 3 : x1 = Extract x1 from Loc1
Step 4 : y1 = Extract y1 from Loc1
Step 5 : For each Device Ni in MDs, do
Step 6 : Loc2 = Extract the Location of Ni from LI
Step 7 : x2 = Extract x2 from Loc
Step 8 : y2 = Extract y2 from Loc
Step 9 : Direct = ""
Step 10 : If (x1 < x2 && y1 < y2) Direct = "NE";
Step 11 : Else If (x1 > x2 && y1 < y2) Direct = "NW";
Step 12 : Else If (x1 > x2 && y1 > y2) Direct = "SW";
Step 13 : Else If (x1 < x2 && y1 > y2) Direct = "SE";
Step 14 : Else If (x1 = x2 && y1 < y2) Direct = "N";
Step 15 : Else If (x1 = x2 && y1 > y2) Direct = "S";
Step 16 : Else If (x1 < x2 && y1 = y2) Direct = "E";
Step 17 : Else If (x1 > x2 && y1 = y2) Direct = "W";
Step 18 : DT = $\sqrt{((x2 - x1)^2 + (y2 - y1)^2)}$ // **Euclidean Distance**
Step 19 : i++
Step 20 : End For
Step 21 : return DirectDist

Algorithm 3: Estimate_Energy_Consumption

Input : Route
Output : Estimated Energy Consumption

Step 1 : EEC = 0
Step 2 : Let Er = k // Er - energy consumption to obtain data
Step 3 : Let Et = k1 // Et - energy consumption for transmitting the data
Step 4 : For each Device Ni in Route, do
Step 5 : Distance = getDistance(Ni, N(i + 1))
Step 6 : EEC = EEC + Er + (Distance * Et)
Step 7 : End For
Step 9 : Return EEC

paths for each MANET device. It then extracts the MEER for each MANET device.

4.2. Cryptographic ensemble approach

This chapter also proposes a cryptographic ensemble approach to protecting soldiers' health parameters data from enemies during data transfer as shown in Figure 4. This approach combines Symmetric Key Encryption using the RC4 algorithm, Identity-Based Encryption (IBE) with Identity Based Signature (IBS). After encryption, it wakes up all available MANET devices in its MEER. If by any means the MANET device senses a soldier's health parameters, it first automatically wakes up and creates a packet. After that, it transmits an encrypted packet through MEER. During MEER packet transfers, the intermediate MANET device keeps a routing table using a Queue format to minimize overheads of routing. Thus the data are quickly transmitted to the control room devoid of any overhead of routing. After getting an ACK message from the Control Room, every MANET node at the MEER path goes to sleep again.

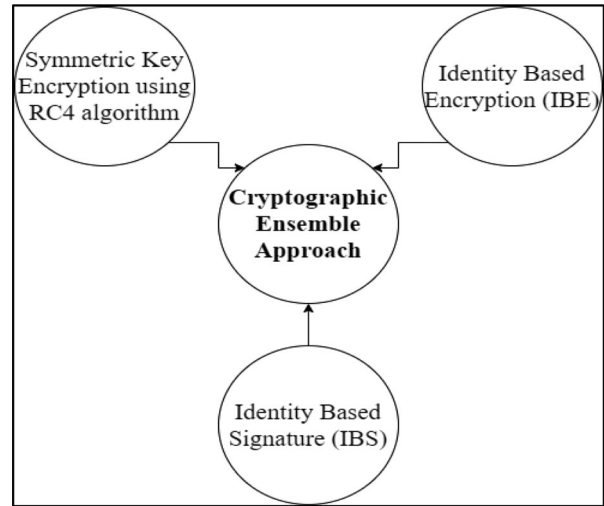


Figure 4. Cryptographic ensemble approach.

After sensing the health parameters of a soldier, the MANET device encrypts health parameters using the RC4 secret key (Symmetric Key Encryption). The resultant of encryption provides Ciphertext1. Followed by it the MANET device encrypts Ciphertext1 using MANET device identity (Identity-Based Encryption). Furthermore, the consequence of encryption provides Ciphertext2. The MANET device generates a signature for Ciphertext2 using MANET device identity based on the HMACSHA-1 algorithm (Identity-Based Signature). Then transmit Ciphertext2 with Signature to the control room through the MEER route. After receiving Ciphertext2 with the Signature, the Control Room officers generate a new signature for Ciphertext2 using MANET device identity based on the HMACSHA-1 algorithm. If the received signature and the unique signature both are the same, they concluded the received Ciphertext2 is safe, otherwise not. After that, they decrypt Ciphertext2 based on the MANET device identity. It provides Ciphertext1.

Furthermore, they decrypt Ciphertext1 based on the sender MANET device RC4 secret key. It gives the original health parameters of a soldier. This workflow is shown in Figure 5.

The proposed cryptographic ensemble approach combines the efficiency of symmetric Key encryption with the convenience of Identity-Based Encryption (IBE) with Identity-Based Signature (IBS). Only users with a secret key and valid Identity can decrypt the data.

To encrypt a message, a fresh secret key is generated and used to encrypt the plaintext data. The sender's identity is used to encrypt the ciphertext once again. The final ciphertext consists of the symmetric ciphertext.

The proposed cryptographic ensemble approach has the following properties:

Secrecy: Except for the length, no one will be able to decipher the encrypted plaintext unless they have access to the secret key and know who sent it.

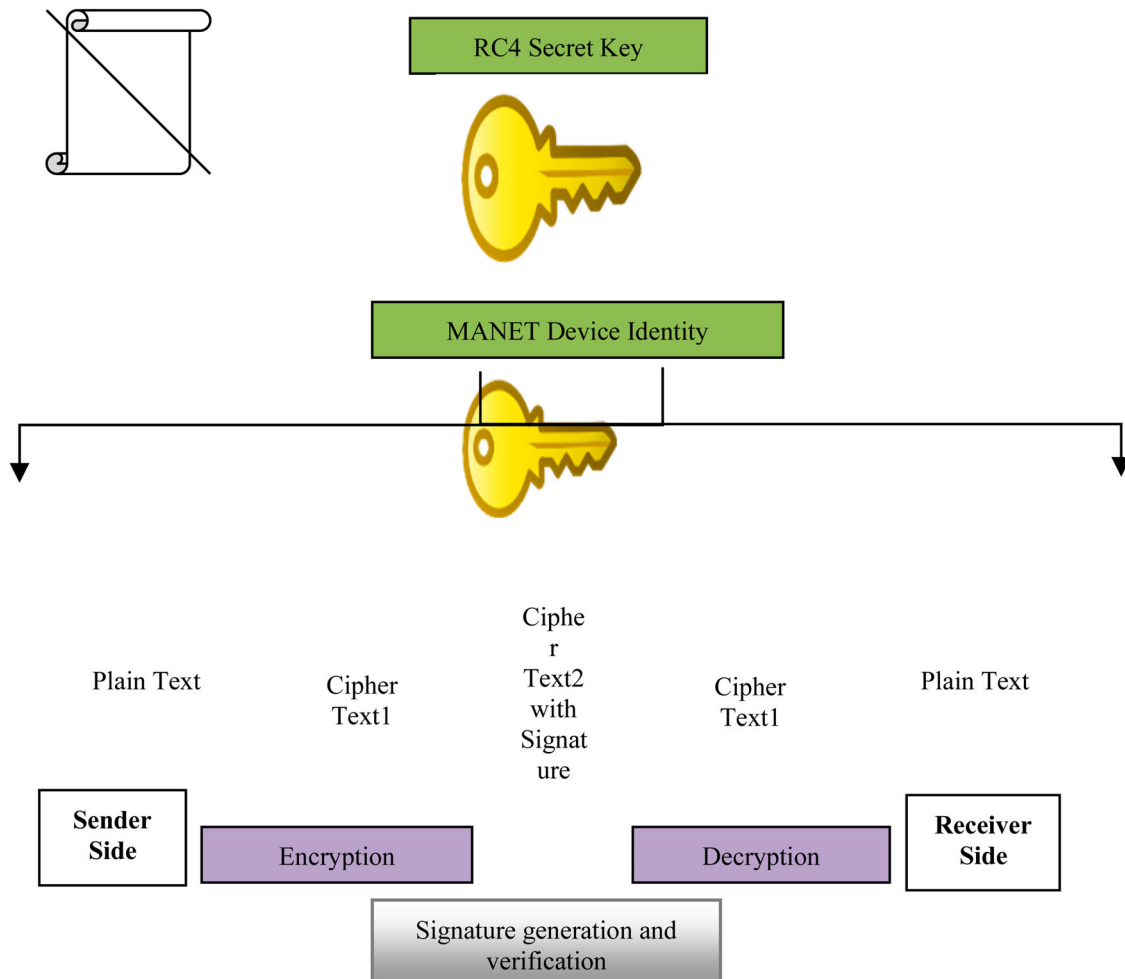


Figure 5. Workflow of cryptographic ensemble approach.

Randomization: The encryption process is random. The ciphertext of two messages with identical plaintext will not match. As a result, attackers are unable to determine which ciphertext matches a certain plaintext.

4.2.1. Symmetric-key encryption using RC4 algorithm

In symmetric-key encryption, the same key is used for both the encryption and the decryption process. The source wants to send the packet to the destination. Therefore, the source wants to encrypt the packet using symmetric key encryption against unauthorized access. So first, it wants to create a secret key based on the key generation phase. This secret key is utilized for both encryptions with decryption. A key represents any code that provides plain text when applied to ciphertext—both the sender and the recipient share this key. If the key is revealed, the confidentiality of the data is compromised. The key is known to the sender and the receiver; hence, it does not protect the sender from the receiver forging a message and claiming the sender sends it. Longer keys are used to increase security and reduce the chances of recognizing the key by brute force. It is relatively fast because it utilizes a similar key

for encryption also decryption. The proposed cryptographic ensemble approach used the RC4 algorithm for symmetric key encryption.

RC4 is a stream cipher with a variable-length key algorithm. It encodes one byte at a time (or bigger units at a time).

A key input is the pseudorandom bit generator, which generates a stream 8-bit number randomly without knowing the input key. The generator's output is known as the key stream, which connects one byte at a time to the plain text stream cipher using the X-OR function.

For instance

RC4 Encryption

$11001000 \text{ (X-OR) } 01010000 = 10011000$

RC4 Decryption

$10011000 \text{ (X-OR) } 01010000 = 11001000$

4.2.2. Identity-based encryption

IBE is a form of public key encryption (PKE) which uses certain identifiers based on the encryption algorithm.

The parties to an IBE conversation can encrypt messages that have no prior-key distribution among them,

which could be helpful when a key distribution is usually inaccessible, technically inaccessible or otherwise.

Utilising an identity ID calculates a public key using the master public key from a Private Key Generator with the ID. It could employ this computed public key to transmit encrypted messages to the entity/person related to the ID.

IBE has quite an extremely simple functioning principle. It permits both the sender and recipient to make a public key from a text value using a recognized identity.

A few of the advantages of IBE are shown as follows:

1. No preparation is needed on the part of the receiver to obtain the encrypted message. It is a very mandatory feature of IBE.
2. No need to manage public key infrastructure, including CRL management.
3. The main benefit of all IBE programs is that if there are merely limited users, following entire users provided by keys the third party's covert could be cleared. It may be because the scheme presumes that the keys are forever suitable once they have been provided (since there is no key revocation mechanism in this basic system).
4. Furthermore, IBE removes the requirement for public key-sharing transportation like public keys resulting from identifiers. The genuineness of public keys is implicitly assured (reliability, integrity and confidentiality) on condition that the transfer of private keys is kept safe for the user concerned.
5. In addition to these features, IBE provides attractive aspects that emerge from the feasibility of encrypting additional data on the identifier. For example, the sender may denote the expiry date of data. He adds this timestamp to the identity of the real receiver (some binary formats such as X.509 may be used). When the recipient communicates with PKG to get back the private key of this public key, PKG could assess the identifier and also reject the removal if it expires. In general, embedded information at an Identity is communicated to open an extra channel between the PKG and the sender, which is assured by a dependence on a private key over the identifier.

4.2.3. Identity-based signature

Digital signatures are the public key primitive of data authentication. They are utilized to bind the signatories of the message. In the world of physics, it is general to employ typed or handwritten messages in handwritten signatures.

Simultaneously, a digital signature is a method which attaches a human being/company to digital information. This attachment could be verified separately through the control room.

A digital signature is a value of encryption computed from information, with a secret key recognized merely through the signer.

Figure 6 shows the Signature generation and verification Workflow.

The Workflows of Signature generation and verification are explained below:

- The sender MANET device inputs the information into the hash operation and also creates the hash of the information.
- The value of the hash with identity is assigned to the signature algorithm that generates the digital signature on the specified hash. The signature will be attached to the packet and after that together will be transmitted to the control room.
- The control room inputs the digital signature with the confirmation key into the confirmation process. The confirmation algorithm provides the result in a few values.
- The control room executes a similar hash operation on the obtained information to create the value of the hash.
- For confirmation, the value of this hash is compared with the yield of the confirmation algorithm. Using the outcome of the comparison, the control room determines whether the digital signature is legitimate or not.

The following section discusses the experimental results and discussion. It evaluates how the proposed MEER algorithm and cryptographic ensemble technique perform.

5. Results and discussions

This section provides the results attained by simulating various situations under various networks and packet sizes. For simulation studies, location awareness of MANET networks is used. Java is utilized for imitation to assess the Cryptographic Ensemble Approach. To assess the routing algorithm, compare the proposed MEER with other popular routing algorithms, such as SHM [27], JILP [27], JRCAR [27], MAXI [27] LECR [27], MEA-DSR [28] and EEPMM [29] using power expenditure, cost of routing, network lifetime, throughput and also delay. Furthermore, to assess the proposed cryptographic ensemble approach, compare the proposed cryptographic ensemble approach with other popular cryptographic algorithms, such as DES [28], AES [29] and Blowfish [30] in terms of encryption and decryption time.

This simulation assumes that 100 MANET devices are identical and that location awareness is distributed over a 900 m with and 600 m height area. The radio transmission range for every device is 100 m, and the early power of the devices is 100 J. Also, the energy

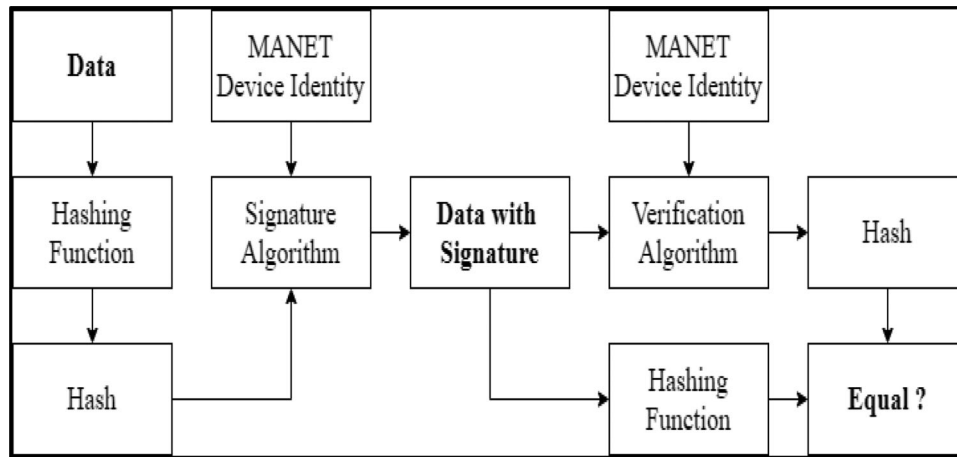


Figure 6. Workflow of signature generation and verification.

threshold for transmitting and receiving a packet is 0.6 J with 0.4 J, respectively. Several runs are made with different device sizes for every situation; also information is gathered for comparison on those runs.

5.1. Metrics for evaluations

The proposed MEER and previous routing algorithms assess effectiveness along with the subsequent metrics:

1. Energy Expenditure
2. Routing Cost
3. Network Lifetime
4. Throughput
5. End-To-End Delay
6. Encryption Time
7. Decryption Time

5.1.1. Energy expenditure

The energy expenditure of each device is calculated when receiving and transmitting. A device that is in sleep mode uses very little energy. The transmission and receiving powers are 0.6 J with 0.4 J, correspondingly. If a device transmits a packet (P) to the subsequent device, the device's power efficiency decreases as shown in Equation (2).

$$EE = RE + (DT * PS * TE) \quad (2)$$

EE is the Energy Expenditure of a device in J; RE is the receiving energy threshold and TE is the transmission energy threshold. DT is the distance from a device to the subsequent device, and PS is the Size of the Packet. In this manner, a device's energy expenditure is computed.

5.1.2. Routing cost

Routing cost is a significant measure of the MANET. Suppose an intermediate device uses 1J in a packet transfer, the routing cost is 0.05 (threshold value). In

Hops	Time
1-5	5 s
5-6	5 s
6-CR	7 s
Total	17 s
Throughput	= 80 kilobits/17 s
	= 4.7 kilobits/s

this manner, the routing cost for the whole route is computed.

5.1.3. Network lifetime

Network lifetime is the most significant effectiveness metric, defined as the time from start to first node failure due to battery power exhaustion.

5.1.4. Throughput

Throughput is a measure of the number of units of information that could be broadcasted in a given time. Its unit is Kilobits/s.

$$TP = TD/TT \quad (3)$$

TP is the Throughput; TD is the Transmitted Data from Source MANET Device to the control room and TT is the Transmission Time.

For example, 10 KB (80 kilobits) data were broadcasted from source MANET Device - 1 to the control room via MEER 1-5-6-CR.

Let

Therefore, Route 1-5-6-CR Throughput for 10 KB data is 4.7 kilobits/s.

5.1.5. End-to-end delay

The time taken for a message transfer from the sender MANET device to the control room is known as the delay. It is a one-way delay.

5.1.6. Encryption time

Encryption time is when it takes for an encryption method to generate a ciphertext from a plaintext.

Table 1. Number of devices versus energy consumption.

No. of devices	SHM	MEA-DSR	EEPMM	MEER
10	60	52	30	21
20	70	65	40	26
30	76	67	45	32
40	80	70	45	33
50	81	71	46	35
60	88	87	52	50
70	90	80	61	56
80	91	83	67	60
90	95	87	73	67
100	96	95	85	72

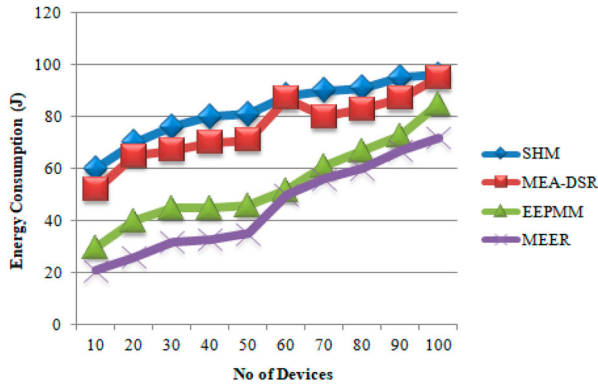


Figure 7. The Number of devices versus energy expenditure.

Encryption time is used to compute the throughput of an encryption scheme. It refers to the speed of encryption.

5.1.7. Decryption time

Decryption time is when it takes a decryption method to generate a ciphertext from a plaintext. Decryption time is used to compute the throughput of a decryption scheme. It refers to the speed of decryption.

5.2. Simulation results

A comparison of different routing algorithms based on the device number and power consumption results is demonstrated in Table 1.

In SHM [27] and MEA-DSR [28], similar devices are utilized for transfers, thus a few chosen devices are often used more times which shorten the lifetime of MANET. Compared with MEA-DSR and SHM, EEPMM [29] uses fewer powers. However compared to EEPMM, the MEER uses little power for the packet transfer, as shown in Figure 7.

Various routing protocols using the device number and routing cost results are shown in Table 2.

The proposed MEER algorithm takes less minimum routing cost, shown in Figure 8, compared to SHM, MEA-DSR and EEPMM [29].

A comparison of various algorithms for routing using network life outcomes is shown in Table 3.

Compared with SHM, MEA-DSR and EEPMM [29], the proposed MEER algorithm network life is longer, as shown in Figure 9.

Table 2. The number of devices versus routing cost.

No. of devices	SHM	MEA-DSR	EEPMM	MEER
10	3	2.6	1.5	1.05
20	3.5	3.25	2	1.3
30	3.8	3.35	2.25	1.6
40	4	3.5	2.25	1.65
50	4.05	3.55	2.3	1.75
60	4.13	3.59	2.57	1.82
70	4.27	3.64	2.62	1.89
80	4.34	3.78	2.74	1.95
90	4.48	3.86	2.89	2.01
100	4.55	3.97	2.96	2.12

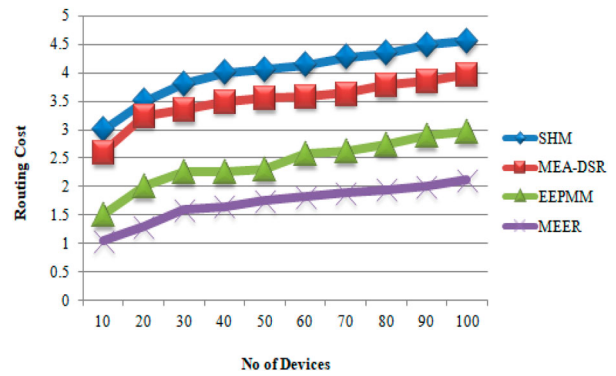


Figure 8. The number of devices versus routing cost.

Table 3. The number of devices versus network lifetime.

No. of devices	SHM	MEA-DSR	EEPMM	MEER
10	350	370	390	430
20	360	380	420	450
30	380	390	410	440
40	390	410	490	540
50	400	420	500	530
60	420	430	510	550
70	450	460	540	570
80	490	510	560	590
90	540	570	600	610
100	590	620	630	660

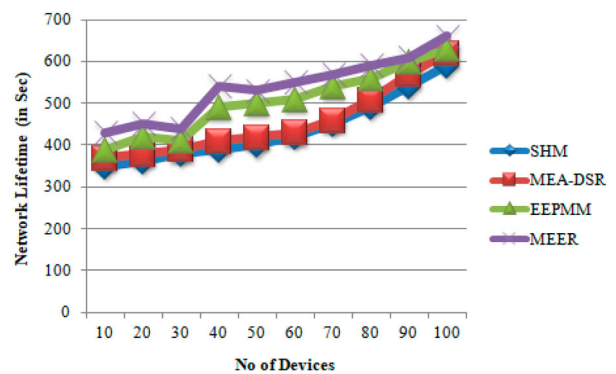


Figure 9. The number of devices versus network lifetime.

A comparison of various algorithms for routing using throughput outcomes is shown in Table 4.

Compared to JILP [27], JRCAR [27], MAXI [27] and LECR [27], the proposed MEER algorithm offers a higher throughput, as shown in Figure 10.

A comparison of various algorithms for routing using end-to-end delay outcomes is shown in Table 5.

Table 4. The number of devices versus throughput.

No. of devices	JILP	JRCAR	MAXI	MEER
10	3630	3490	3490	3520
20	3340	3280	3310	3340
30	2740	2910	2910	2920
40	2290	2430	2510	2870
50	1910	2080	2170	2430
60	1970	1980	2110	2220
70	1500	1910	1970	2100
80	1490	1500	1620	1790
90	1300	1440	1570	1730
100	1280	1390	1390	1430

Compared with JILP [27], JRCAR [27], MAXI [27] and LEQR, the proposed MEER takes fewer delays, as shown in Figure 11.

To evaluate cryptographic algorithms, compare the proposed cryptographic ensemble approach with other popular cryptographic algorithms, such as DES [28], AES [29] and Blowfish [30]. Table 6 shows the comparison of various cryptographic algorithms based on encryption time with various transmissions.



Figure 10. The number of devices versus throughput.

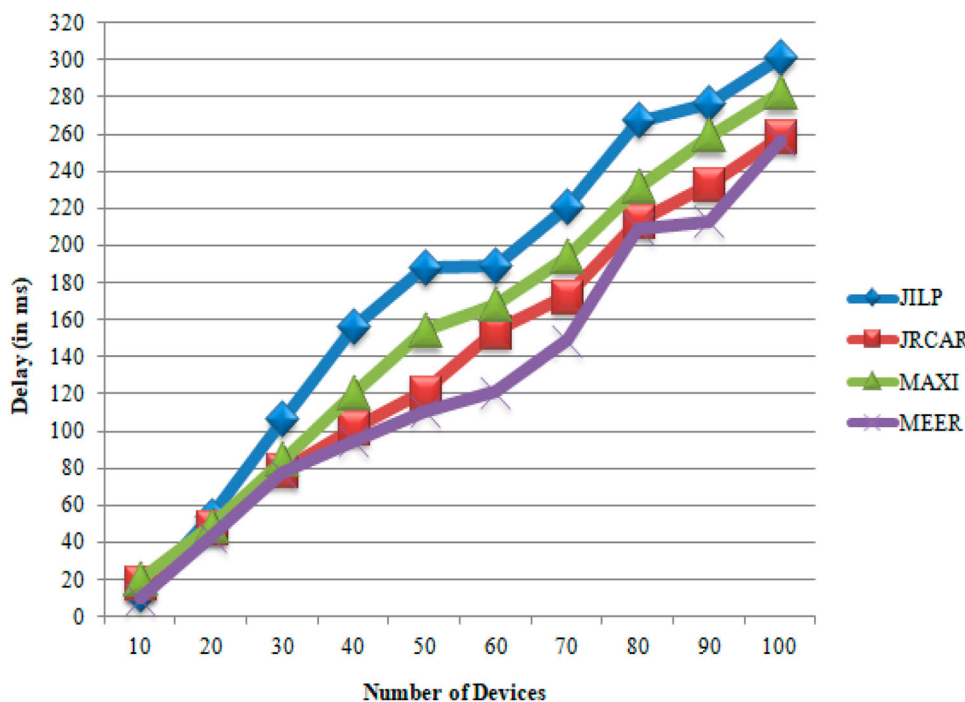


Figure 11. The number of devices versus delay.

Table 5. The number of devices versus delay.

No. of devices	JILP	JRCAR	MAXI	MEER
10	12	19	20	10
20	54	48	49	43
30	106	79	84	78
40	156	102	120	95
50	188	121	154	111
60	189	154	168	121
70	221	173	194	149
80	267	213	231	209
90	276	233	259	213
100	301	259	282	257

Table 6. Encryption time-based comparison of various cryptography algorithms.

Transmission Id	DES	AES	Blowfish	Cryptographic ensemble approach
Transmission - 1	22	15	9	7
Transmission - 2	27	24	15	12
Transmission - 3	24	19	21	14
Transmission - 4	31	29	25	16

Table 7. Decryption time-based comparison of various cryptography algorithms.

Transmission Id	DES	AES	Blowfish	Cryptographic ensemble approach
Transmission - 1	15	18	14	12
Transmission - 2	16	19	15	11
Transmission - 3	29	23	24	18
Transmission - 4	24	19	22	16

Compared to DES, AES and Blowfish, this proposed cryptographic ensemble technique takes less time for encryption, as shown in Figure 12.

Table 7 shows a comparison of various cryptographic algorithms using decryption time during other transmissions.

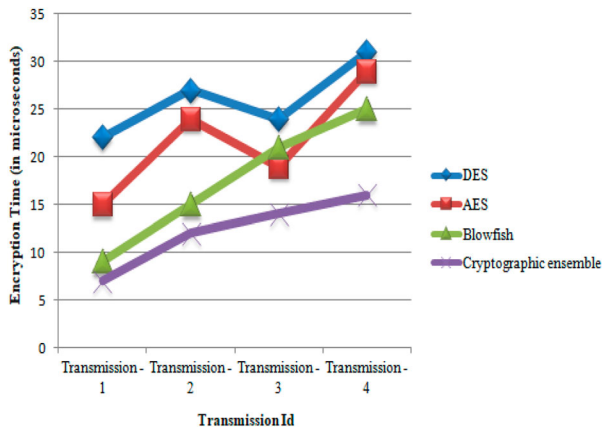


Figure 12. Comparison of encryption time.

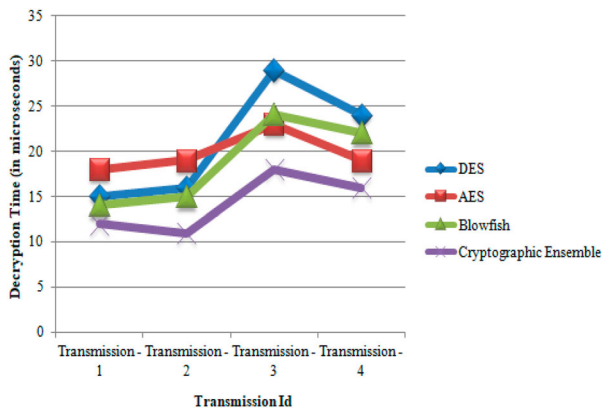


Figure 13. Decryption time comparison.

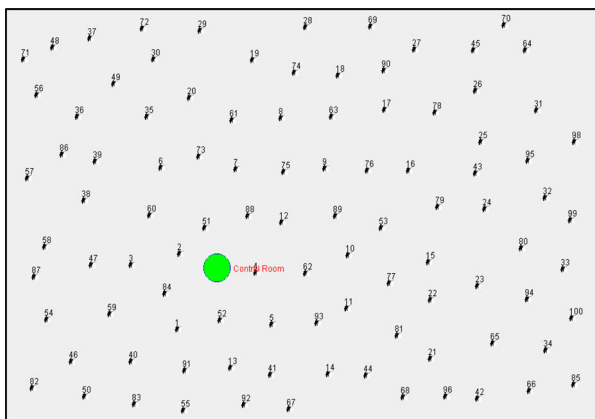


Figure 14. MANET network with one control room and 99 MANET devices.

This proposed cryptographic group approach to decryption is shown in Figure 13 compared to DES, AES and Blowfish.

5.3. Sample scenarios

Figure 14 demonstrates a Network of MANET. It has one Control Room and 99 MANET nodes.

Figure 15 shows the Minimum Energy Expenditure Route from MANET Device – 49 to the Control room.

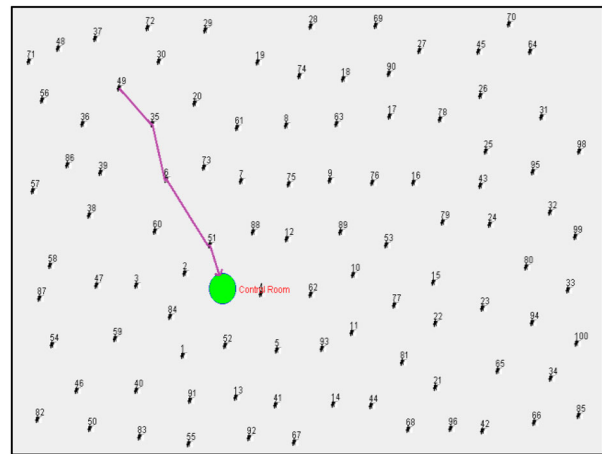


Figure 15. Minimum energy expenditure route.

6. Conclusion

This paper presented an algorithm for routing called Minimum Energy Expenditure Routing (MEER). It used to sleep with wakefulness planning for entire MANET devices to solve the big energy expenditure problems and find the entire obtainable paths using Euclidean distance by direction findings. In addition, it discovers the minimum power consumption path using the estimated power Expenditure algorithm. The MEER algorithm decreased the overhead of routing based on the Maintenance of the Routing Table and First-in-First-Out. This paper presented a cryptographic ensemble approach that ensembles three cryptography techniques, namely symmetric key encryption using the RC4 algorithm, IBE, with IBS. This approach provides the security of the health parameter of soldiers while data transmission from the soldier to the control room. Furthermore, the cryptographic ensemble approach offers strong protection and takes less time for both encryption and decryption. Finally, the experimental result showed that the proposed MEER algorithm reduced energy consumption, routing cost and end-to-end delay and also increased network lifetime and throughput than other existing routing algorithms. Furthermore, it showed that compared with other popular cryptographic algorithms the proposed cryptographic ensemble approach takes less time for encryption and decryption.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This study did not receive any funding in any form.

ORCID

B. V. V. Siva Prasad <http://orcid.org/0000-0001-8650-3984>
 Sridhar Mandapati <http://orcid.org/0000-0001-7649-499X>
 Lakshmana Kumar Ramasamy <http://orcid.org/0000-0002-0643-6599>

Rajasekhar Boddu  <http://orcid.org/0000-0002-2522-206X>
 Pranayanath Reddy  <http://orcid.org/0000-0002-4103-5539>
 B. Suresh Kumar  <http://orcid.org/0000-0001-5864-1634>

References

- [1] Bandopadhyaya S, Dey R, Suhag A. Integrated healthcare monitoring solutions for soldier using the internet of things with distributed computing. *Sustain Comput Inf Syst.* **2020**;26:100378.
- [2] Mathavan V, Nanthini N, Chinnapparaj S, et al. War field soldier body condition monitoring system. *Mater Today Proc.* **2021**;37:2798–2802.
- [3] Albahri OS, Albahri AS, Mohammed KI, et al. A systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: taxonomy, open challenges, motivation and recommendations. *J Med Syst.* **2018**;42(5):1–27.
- [4] Sharma PK, Park J, Park JH, et al. Wearable computing for defence automation: opportunities and challenges in 5G network. *IEEE Access.* **2020**;8:65993–66002.
- [5] Razzak MA, Islam MN. Exploring and evaluating the usability factors for military application: A road map for HCI in military applications. *Human Factors Mech Eng Defense and Safety.* **2020**;4(1):1–18.
- [6] Deepa J, Sutha J. A new energy-based power-aware routing method for MANETs. *Cluster Comput.* **2019**;22(6):13317–13324.
- [7] Karthikeyan MM, Dalin G. Dynamic congestion control routing algorithm for energy harvesting in MANET. In: *Inventive computation and information technologies: Proceedings of ICICIT 2020.* Singapore: Springer; **2021.** p. 15–25.
- [8] Robinson YH, Krishnan RS, Julie EG, et al. Neighbour knowledge-based rebroadcast algorithm for minimising the routing overhead in mobile ad-hoc networks. *Ad Hoc Netw.* **2019**;93:101896.
- [9] Malar ACJ, Kowsigan M, Krishnamoorthy N, et al. Multi constraints applied energy-efficient routing technique based on ant colony optimisation used for disaster resilient location detection in a mobile ad-hoc network. *J Ambient Intell Humaniz Comput.* **2021**;12:4007–4017.
- [10] Saba T, Haseeb K, Ahmed I, et al. Secure and energy-efficient framework using internet of medical things for e-healthcare. *J Infect Public Health.* **2020**;13(10):1567–1575.
- [11] Chen Z, Zhou W, Wu S, et al. An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. *IEEE Access.* **2020**;8:44760–44773.
- [12] Khudayer BH, Anbar M, Hanshi SM, et al. Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. *IEEE Access.* **2020**;8:24019–24032.
- [13] Li T, Ma J, Pei Q, et al. DAPV: Diagnosing anomalies in MANETs routing with provenance and verification. *IEEE Access.* **2019**;7:35302–35316.
- [14] Zhang T, Zhao S, Cheng B. Multipath routing and MPTCP-based data delivery over manets. *IEEE Access.* **2020**;8:32652–32673.
- [15] Khan MA, Ullah I, Nisar S, et al. An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network. *IEEE Access.* **2020**;8:36807–36828.
- [16] Elhoseny M, Shankar K. Reliable data transmission model for mobile ad hoc network using signcryption technique. *IEEE Trans Reliab.* **2019**;69(3):1077–1086.
- [17] Farouk F, Alkady Y, Rizk R. Efficient privacy-preserving scheme for location-based services in VANET system. *IEEE Access.* **2020**;8:60101–60116.
- [18] Anbarasan M, Prakash S, Antonidoss A, et al. Improved encryption protocol for secure communication in trusted MANETs against denial of service attacks. *Multimed Tools Appl.* **2020**;79(13):8929–8949.
- [19] Shukla M, Joshi BK. WITHDRAWN: “A novel approach using elliptic curve cryptography to mitigate Two-Dimensional attacks in mobile Ad hoc networks”. *Mater Today Proc.* **2021.**
- [20] Elmahdi E, Yoo SM, Sharshembiev K. Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. *J Inf Security Appl.* **2020**;51:102425.
- [21] Muruganandam S, Renjit JA. Real-time reliable clustering and secure transmission scheme for QoS development in MANET. *Peer-to-Peer Network Appl.* **2021:** 1–16.
- [22] Khanna N, Sachdeva M. A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and their variants in MANETs. *Comput Sci Rev.* **2019**;32:24–44.
- [23] Thiagarajan R, Ganesan R, Anbarasu V, et al. Optimised with the secure approach in detecting and isolating malicious nodes in MANET. *Wirel Pers Commun.* **2021:** 1–15.
- [24] Abebe AT, Shiferaw YN, Kumar PS. Efficient reconfigurable integrated cryptosystems for cybersecurity protection. In: *Advances in cyber security analytics and decision systems.* Cham: Springer; **2020.** p. 57–77.
- [25] Mahamune AA, Chandane MM. TCP/IP layerwise taxonomy of attacks and defence mechanisms in mobile Ad Hoc networks. *J Inst Eng (India): Ser B.* **2021:** 1–19.
- [26] Suma R, Premasudha BG, Ram VR. SIBLAR: a secured identity-based location-aware routing protocol for MANETs. *Int J Comput Aided Eng Technol.* **2021**;14(3):320–344.
- [27] Medeiros VN, Silvestre B, Borges VC. Multi-objective routing aware of mixed IoT traffic for low-cost wireless backhauls. *J Internet Serv Appl.* **2019**;10(1):1–18.
- [28] Quist-Aphetsi K, Xenya MC. Securing medical IoT devices using Diffie-Hellman and DES cryptographic schemes. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT);* 2019, May (pp. 105–108). IEEE. 29-31 May 2019. Accra, Ghana.
- [29] Khader M, Alian M, Hraiz R, et al. Simplified AES algorithm for healthcare applications on internet of thing. In: *2017 information technology (ICIT).* IEEE; **2017, May.** p. 543–547.
- [30] Kondawar SS, Gawali DH. Blowfish algorithm for patient health monitoring. *2016 International Conference on Inventive Computation Technologies (ICICT)* (Vol. 3, p. 1–6); 2016 August. IEEE. 26-27 August 2016, Coimbatore, India.
- [31] Shen T, Wang F, Chen K, et al. Efficient leveled (multi) identity-based fully homomorphic encryption schemes. *IEEE Access.* **2019**;7:79299–79310.
- [32] Rango FD, Lonetti P, Marano S. MEA-DSR: A multipath energy-aware routing protocol for wireless Ad Hoc networks. *IFIP Annual Mediterranean Ad Hoc Networking Workshop* Boston, MA: Springer; **2008.** p. 215–225.
- [33] Sun B, Lu M, Xiao K, et al. An energy entropy-based minimum power cost multipath routing in MANET. *Int J Grid Distrib Comput.* **2016**;9(2):169–180.