applied sciences

MDPI

Article

Data Security-Based Routing in MANETs Using Key Management Mechanism

Praveen Bondada [1,†], Debabrata Samanta [1,2,†], Manjit Kaur [3,†] and Heung-No Lee [3,*,†]

1 Dayananda Sagar Research Foundation, University of Mysore (UoM), Mysuru 570005, India; praveen071205@gmail.com (P.B.); debabrata.samanta369@gmail.com (D.S.)
2 Department of Computer Science, CHRIST University, Bangalore 560029, India
3 Gwangju Institute of Science and Technology, School of Electrical Engineering and Computer Science, Gwangju 61005, Korea; Manjitbhinder8@gmail.com
* Correspondence: heungno@gist.ac.kr
† These authors contributed equally to this work.

Abstract: A Mobile Ad Hoc Network (MANET) is an autonomous network developed using wireless mobile nodes without the support of any kind of infrastructure. In a MANET, nodes can communicate with each other freely and dynamically. However, MANETs are prone to serious security threats that are difficult to resist using the existing security approaches. Therefore, various secure routing protocols have been developed to strengthen the security of MANETs. In this paper, a secure and energy-efficient routing protocol is proposed by using group key management. Asymmetric key cryptography is used, which involves two specialized nodes, labeled the Calculator Key (CK) and the Distribution Key (DK). These two nodes are responsible for the generation, verification, and distribution of secret keys. As a result, other nodes need not perform any kind of additional computation for building the secret keys. These nodes are selected using the energy consumption and trust values of nodes. In most of the existing routing protocols, each node is responsible for the generation and distribution of its own secret keys, which results in more energy dissemination. Moreover, if any node is compromised, security breaches should occur. When nodes other than the CK and DK are compromised, the entire network's security is not jeopardized. Extensive experiments are performed by considering the existing and the proposed protocols. Performance analyses reveal that the proposed protocol outperforms the competitive protocols.

Keywords: cryptosystems; MANET; routing; security; key management

Citation: Bondada, P.; Samanta, D.; Kaur, M.; Lee, H.-N. Data Security-Based Routing in MANETs Using Key Management Mechanism. *Appl. Sci.* **2022**, *12*, 1041. https://doi.org/10.3390/app12031041

Academic Editor: Arcangelo Castiglione

Received: 11 December 2021
Accepted: 17 January 2022
Published: 20 January 2022

1. Introduction

Mobile Ad Hoc Networks (MANETs) are autonomous networks developed using wireless mobile nodes without the support of any kind of infrastructure. In a MANET, nodes can communicate with each other freely and dynamically through radio frequencies [1–3]. MANETs allow mobile users to communicate with one another when permanent infrastructure is not available or possible [4]. The routes in a MANET are frequently unable to work correctly due to external noise, transmission interference, and mobility. The development of the internet in recent years has considerably improved MANETs' usage in various critical applications. Recently, MANETs are extensively utilized to build Internet of Things (IoT)-based smart networks [5,6]. As a result, the requirements for safety and consistency in these types of networks should be thoroughly re-evaluated.

Due to a limited transmission range, nodes communicate with each other using multiple hops [7]. Thus, the availability of every node is equally important. Therefore, an efficient routing protocol is required to evaluate an optimal path between the source and sink.

While developing a MANET, many routing protocols based on trust were suggested and evaluated. Most trusted management plans were built for cooperative routing to

detect the self-destructive nodes caused by erroneous nodes. When developing safer route protocols, researchers have considered reputations and links about mobile nodes, among other things. Various predicted route models were also designed, which were used to quantitatively identify distinct types of security assaults. Some researchers discussed the issues related to key problems associated with the IoT-based MANETs. Various security and vulnerability risks were considered during the design of protocols [8,9]. The routing protocols can be categorized as reactive, proactive, and hybrid. The proactive routing protocols, such as the Destination Sequence Distance Vector (DSDV) [10], need periodic updates of the routing tables. Thus, a huge number of control packets are generated. Hence, these protocols were found to be unsuitable for MANETs. Therefore, reactive protocols, such as ad hoc on-demand distance vector routing (AODV) [11] and dynamic source routing (DSR) [12], were designed. A path is developed between the source and sink whenever it is required.

These protocols utilize two steps, i.e., route discovery and route maintenance. Routes are computed using a route-discovery process. A source node utilizes a route-maintenance step to evaluate any changes in topology. To secure communication among MANET nodes, various cryptography-based protocols have been proposed. Some well-known protocols are Efficient Node Admission and Certificateless Secure Communication (ENACSC) [13], Anonymous Location-Aided Routing (ALARM) [14], Energy-Efficient Partial Permutation Encryption (EEPPM) [15], Friend-Based Ad Hoc Routing to Establish Security (FACES) [16], Anonymous Multipath Routing Protocol (AMRP) [17], Statistical Traffic Pattern-Discovery System (STARS) [18], and Non-Interactive Self-Certification (NSC) [19]. However, these protocols are prone to various security threats and also consume more energy from the nodes. In [20], a trust-based approach with efficient predictability for MANETs on the IoT was designed; it estimates the last node value based on direct and indirect information judgments and a sense of trust . In [21], an energy consumption system was designed for MANETs on the IoT that was based on ant colony optimization. Ant colonies were used to minimize the end-to-end delay.

Recently, many secure and energy-aware multipath routing protocols have been designed for MANETs, such as the Trust Aware Secure Energy Efficient Hybrid Protocol (TASEEHP) [22], Hybrid Secure Multipath Routing Protocol (HSMRP) [23], Signcryption Technique (ST) [24], and Recurrent Reward-Based Learning (RRBL) [25]. These protocols have shown remarkable performance against various security threats. Although these protocols consume less energy than the existing protocols, there is still room for energy conservation.

1.1. Motivation

For secure communication in MANETs, various secret keys are used. In most of the existing cryptography-based routing protocols, each node is responsible for the generation and distribution of its own secret keys. The main objective of this paper is to prevent energy dissipation due to the individual key generation and distribution. Therefore, an efficient energy-aware secure key management system is proposed. Asymmetric key cryptography is used, which involves two specialized nodes, labeled Calculator Key (CK) and Distribution Key (DK). These two nodes are responsible for the generation, verification, and distribution of secret keys. As a result, other nodes need not perform any kind of additional computation for building the secret keys. These nodes are selected using the energy consumption and trust values of nodes.

1.2. Contributions

The main contributions of this paper are as follows:

- An efficient and energy-aware secure key management system is proposed, using two specialized nodes labeled Calculator key (CK) and Distribution key (DK);
- These two nodes, i.e., CK and DK, are responsible for the generation, verification, and distribution of secret keys;

- The energy and trust factors of MANET nodes are utilized for the selection of these nodes, i.e., CK and DK;
- Extensive experiments are performed for the verification and validation of the proposed secure key management system.

The remaining paper is organized as follows: Section 2 presents the proposed methodology. The selection of the Calculator Key (CK)- and the Distribution Key (DK)-based secure communication framework is presented in Section 3. Section 4 presents the simulation environment and performance metrics used for comparative analysis. Experimental results and a comparative analysis are presented in Section 5. Concluding remarks are discussed in Section 6.

2. Proposed Model

This section discusses the proposed trust-management system. The following sections outline the trust-management processes. The proposed method initially establishes a network and initializes the source node. The suggested approach then collects data from the subsequent log reports to see the packets' positive or negative rates between the nodes. The AODV protocol is used as a base protocol.

2.1. Ad Hoc On-Demand Distance Vector

In AODV, the use of destination sequence numbers prevents the problem of counting to infinity. As a result, the AODV loop has been removed. Route Errors (RERRs) are used to warn the network of a route's connection failure, whereas Route Replies (RREPs) are used to complete the routes. Three different types of messages can be used to define AODV [26]. To begin the route-finding process, Route Requests (RREQs) are utilized. To complete the process, RREPs are employed.

It is necessary for each node to keep two different counters, i.e., one for the number of nodes in the sequence and the other for broadcast ID. As shown in Figures 1 and 2, when the source node broadcasts an RREQ packet to its neighbors to start the path discovery, it maintains a record of the consequent information. This information is required to instrument both the reverse-path setup and the forward-path configuration that is used in conjunction with the transmission protocol (RREP). An RREQ has two sequence numbers, one of which is the source sequence number, and one that is the last known destination sequence number [5].

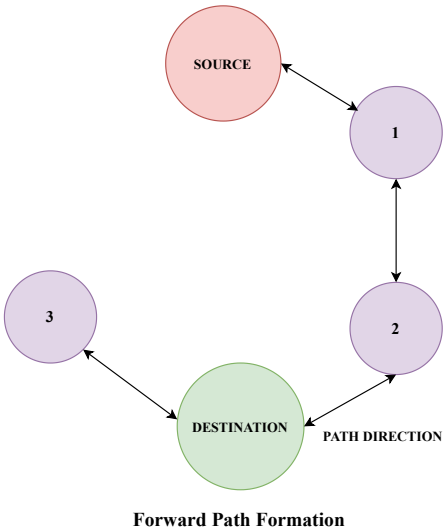

Figure 1. Forward-path formation.

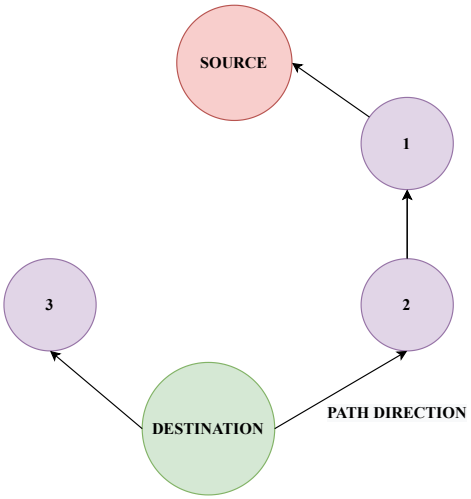

Figure 2. Reverse-path formation.

2.2. Trust Management

It is possible to predict the trust value by comparing the packet sequence ID of the nodes using log reports. AODV is a receptive routing protocol that organizes routes whenever the destination sequence numbers are necessary for the most recent route to acquire. This functionality allows AODV to operate an updated route to the destination. However, the projected destination nodes are less reliable due to malicious behavior. Thus, the trust value is computed using the cryptographic function, hybrid energy assessment, packet-delivery success rate, mobility, and location key calculation.

Initially, nodes with the largest trust values are selected for packet transfer. These evaluations make the identified route credible and secure with a high confidence value. Figure 3 shows the flow diagram of the proposed technique.

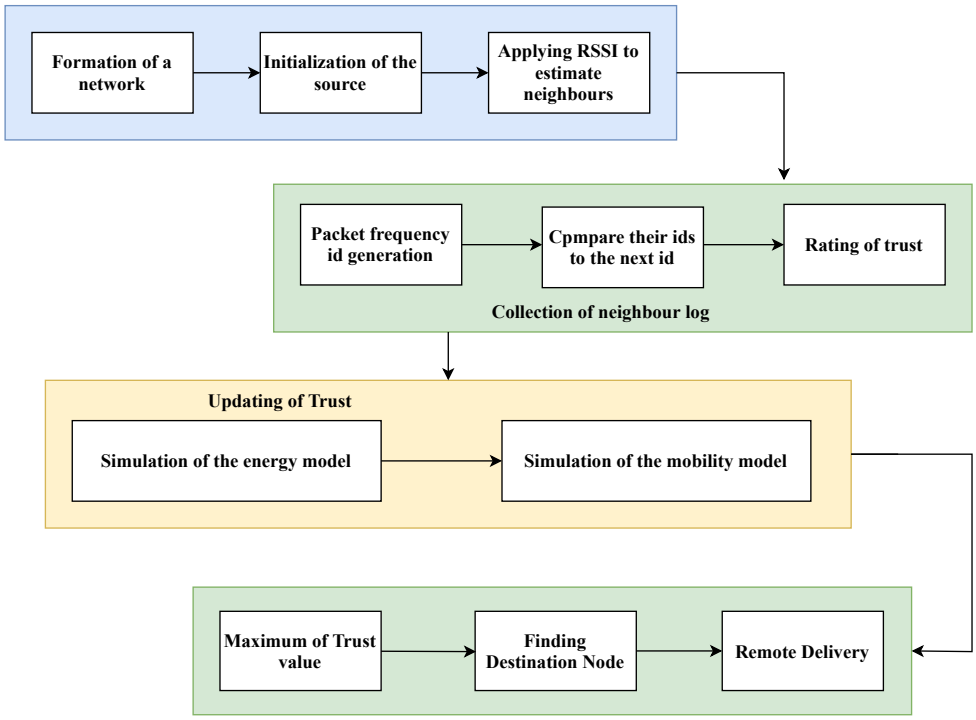

Figure 3. Flow diagram of the proposed technique.

Additionally, a Received Signal Strength Indicator (RSSI) is used to determine wether the selected trust node lies within the communication range, as nodes can travel in any direction and operate as both hosts and routers [27].

2.3. Mobility-Based Model Function

Mobile node movement is often referred to as the mobility function. It contains the speed and direction of the node. The distance between the nodes can be calculated by utilizing a constant k and the required transmission/receiving power:

$$e = \sqrt[4]{j \cdot \frac{tr}{ts}} \tag{1}$$

Here, e defines the mobility function, j shows the mobility constant, tr and ts show the time for the first node's traveling distance and traveling speed, respectively, and r represents the traveling distance.

The neighbor speed (w) can be computed as:

$$w = \frac{\Delta e}{\Delta r} \tag{2}$$

The level of the neighboring node in relation to the selected node primarily depends on the speed constraint. The following condition is used:

$$\text{Direction } = \begin{cases} \bar{w} > 0. \text{ onside} \\ \bar{w} = 0. \text{ fixed} \\ \bar{w} < 0. \text{ inside} \end{cases} \tag{3}$$

Here, $\bar{w}$ shows the direction of the nodes.

The mobility function can be defined as:

$$M_i = VTR_i + e \tag{4}$$

where M_i defines the mobility of ith node, VTR_i represents the velocity transmission rate of ith node, and e shows the obtained mobility value using Equation (1).

2.4. Energy Function Computation

The energy function defines the energy consumed by nodes during the data-transmission process. Road maintenance and neighbor-sensing are the main responsibilities of the energy model. It can be calculated as follows:

$$F_{n,o} = [(qk_{n,o} \times qs_{n,o}) + (qs_{n,o} \times rs_{n,o}) + (qr_{n,o}rs_{n,o})] \tag{5}$$

Here, $F_{n,o}$ shows the total energy function, $qk_{n,o}$ shows the energy required by the kth node, $qs_{n,o}$ defines the energy required for the sth node, $qr_{n,o}$ defines ther energy required for rth node, and $Vs_{n,o}$ shows the energy required for root identification. After the selection of a trustworthy node to transmit the packet, its energy dissemination should be updated for further transmission of the packets. The total energy (Eim, n) can be simplified as follows:

$$Fk_{n,o} = Fk_{n,o} - F_{n,o} \tag{6}$$

Here, $Fk_{m,o}$ shows the energy function of the second iteration. $F_{n,o}$ shows the energy function of the first iteration.

The trust value ($TC_{t,k}$) can be estimated by using the computed trust, energies, and mobility values as follows:

$$TC_{t,k} = F_{t,k} + TR_i - N_i \tag{7}$$

Here, $F_{t,k}$ shows the trust factor, k defines the secret key, TR_i shows the transmission distance of the ith node, and N_i represents the mobility of ith node.

A node with the largest trust value is selected for the data transmission. The route discovery must be done once the destination is reached or the neighbor's estimation must be done again. The network's route between a source node and nearest neighboring nodes is evaluated using the proposed trust model. If the distance between the source and the nearest node falls within the coverage region, the current node's information is added to the list of neighboring nodes. The log report for the estimated neighbor node is obtained for further analyses.

2.5. Cryptographic Methods

Recently, many cryptography approaches have been proposed for securing MANETs and IoT networks [28]. The objective is to provide secure data communication. In this paper, a source node finds the CK and DK nodes in the routing table to evaluate the secure routes. Validation, encryption, and trust are all achieved through cryptographic calculations [29–31]. The majority of cryptographic frameworks necessitate a key management mechanism that is safe, dynamic, and efficient. Any protected communication system relies on the management of keys. The proposed approach uses strong encryption algorithms to provide secure data delivery. The main process of the selection of CK and DK nodes is presented in Section 3.1.

3. Secure Data Communication Framework

The proposed secure data communication framework for MANETs depends upon the Calculator Key (CK) and Distribution Key (DK). The remaining section discusses the calculation of the CK and DK and how they provide security to MANETs.

3.1. Selection of the Calculator Key (CK) and Distribution Key (DK)

Initially, the network assigns energy levels to each node in its system. The CK and DK nodes are evaluated by following the route discovery, using residual activity levels and route-critical nodes. The CK node generates keys, i.e., public and private keys, and provides them to the DK. The goal of the CK is to obtain secret key pair variables and communicate only the set key to DK. Before the keys are distributed, all nodes in the network connection must be registered with the DK node, which verifies the node's validity. Figure 4 shows the selection of the CK and DK.

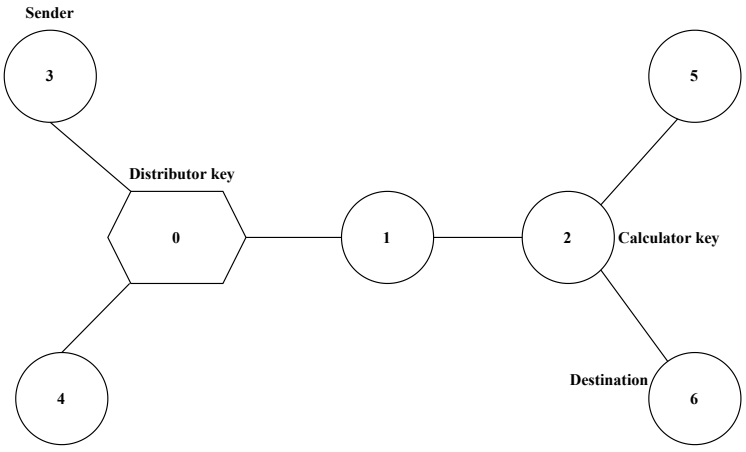

Figure 4. Selection of the Calculator Key (CK) and Distribution Key (DK).

Figure 5 shows the flow of a key distribution process. Initially, the CK generates a key pair set and makes it broadly available for the DK. Thereafter, the DK distributes the keys

to the registered nodes. The following approach is used to create key pairs that contain both public and private keys. Take two numbers that are primary l and p:

$$\begin{aligned} PUR &= l \times p \\ \Theta(R) &= (l-1)(p-1) + l + p \\ H(j) &= \Theta(R) + (l\&p) \\ PUB(R_i) &= H(R)\&l\&p + PUK \end{aligned} \tag{8}$$

where PUR defines the product of two nodes, $H(j)$ shows the functions for generating the public key, $\Theta(R)$ defines the node-to-node distance for small values, and $H(R)$ is a function of the modified node value.

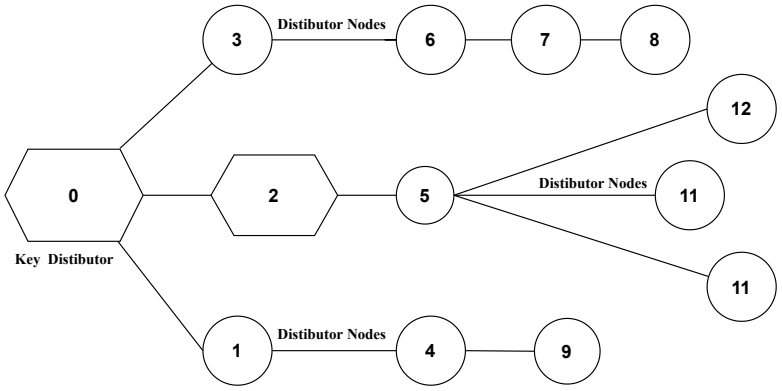

Figure 5. Flow of the key distribution process.

Generation of the Private Key

For the generation of a private key KC, integer numbers $w_1, w_2, ..., w_o$ are assumed to be 1 in the first and last Greatest Common Divisor (GCD) numbers. Consider a new number set, $n_1, n_2, ..., n_o$:

$$\begin{aligned} &\mathrm{R} \equiv n_1(\mathrm{mod}\, w_1) \\ &\mathrm{R} \equiv n_2(\mathrm{mod}\, w_2) \ldots \mathrm{R} \equiv n_{\mathrm{o}}(\mathrm{mod}\, w_{\mathrm{o}}) \\ &\mathrm{R} = n_1\mathrm{q}1\mathrm{R}1 + n_2\mathrm{q}2\mathrm{R}2 + \ldots\ldots\ldots + n_0\mathrm{q}_0\mathrm{R}_0 \\ &\mathrm{T_i} = \mathrm{V_i}/n_{\mathrm{k}}, \mathrm{q_k} = \mathrm{T_k} - l(\mathrm{mod}\, n_{\mathrm{k}}) \\ &\mathrm{PRK}(\mathrm{R_k}) = \mathrm{T_k} \times \mathrm{PUB}(\mathrm{R_k}) - l - \mathrm{p} - \mathrm{PUR}. \\ &\mathrm{KeyPair(RP)} = \mathrm{set}\{\mathrm{PUB}(\mathrm{K_k}) : \mathrm{PUR}(\mathrm{R_k})\} \end{aligned} \tag{9}$$

Here, R represents the distance between both key nodes, PRK shows the private key, PUB shows public key, T_i shows the trust value of the ith node, R_K is a modified private key, q shows the various functions required for the generation of PUB, and V_i represents a velocity of transmission distance for the ith node.

The DK receives the key pairs once they have been generated. The public key from the DK is requested based on the routing information of the source node whenever communication is started. The DK searches the routing database for the key and sends it to the encryption unit. Based on the routing table's information, the actual amount of data is divided into data packets and supplied to neighboring nodes (refer to [32,33]). If data is received by the destination node, a request is made to forward the source node ID to the private key. The DK analyzes the destination as legitimate or not and then transfers the data-decryption privacy key to the target node. Figure 6 demonstrates the proposed data-communication framework.

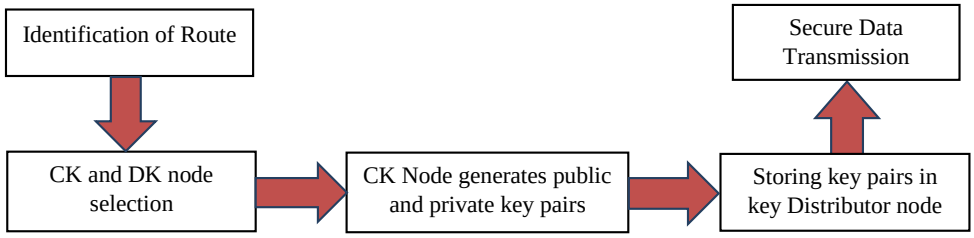

Figure 6. Proposed data-communication framework.

3.2. Secure Data-Communication Framework

Instead of sending harmful data packets to the next hop, these packets can be dropped completely or partially received. The initial communication between the source and the target nodes is made to discover malicious nodes (refer [34,35]). The trust value for every node is derived using fluctuating criteria, ranging from 0 to 1. Each node has a common threshold value, and each network node may be identified by utilizing the threshold value either as a compromised node or a regular node. Identified malicious nodes are removed from the network by altering the state power. The source node can select a reliable path to its target node if the malicious nodes between the source and destination nodes are already removed.

The proposed model utilizes asymmetric key cryptography, and two specialized nodes, CK and DK, are utilized. These two nodes are used for key generation and verification. Thus, all other nodes in the network need not make any other computations. This will help us to save the energy of nodes. Here, the CK and DK nodes are selected based on their energy and trust factors. The secret keys are distributed to other nodes using the DK. In most of the existing models, every node needs to generate its own keys. Thus, every node spends its energy on key-generation and key-distribution processes. Moreover, if any node is compromised, it will result in security breaches. In the proposed approach, if any node other than the CK and DK is compromised, it will not affect the security of the entire network.

4. Simulation Environment and Performance Metrics

This section discusses the simulation environment and performance metrics used for comparative analyses.

4.1. Simulation Environment

The proposed model is implemented on the NS2.33 simulator using Ubuntu 16.04. Initially, the existing C++ code is modified to implement the trust-based scheme. Thereafter, various scenarios are generated and implemented in Tool Command Language (TCL) to run the simulation. The source code mainly involves a hello packet and the transmission of receiving RREQ and RREP packets (refer [36,37]). Hello packets are used to carry the values of the parameters needed to work out on the dynamic trust of the neighbor node, while the RREQ and RREP packets are used to carry the trust values for mutual authentication. RREQ packets are used to request and RREP packets are used to send the trust value between communicating pair nodes. The simulation is achieved by using online libraries and by re-using code, modifying the AODV member functions. The modified code allows the AODV to carry the trust information (refer [38,39]). NS2 script is used to build the network scenario and CBR is used as a traffic generator. A number of nodes, speeds, cover areas, and simulation times are used as parameter types to test the proposed scheme. A wireless channel, using 802.11 as the MAC protocol, is used to run the proposed scheme. Table 1 shows the simulation parameters.

Table 1. Simulation parameters.

Parameters	Value
Number of nodes	5–60 nodes
Packet size	1000 byte
Radio range	150 m
Area	500 m × 500 m
Number of traffic sources	4
Pause time(s) at simulation	I0 s
Traffic type	CBR
Send rate of traffic	4 packets/second
Routing Protocol	AODV
Mobility model	Random Waypoint Mobility [40]
Data rate	11 Mbps
Simulation Time	100 s

4.2. Malicious Nodes

Nodes that intentionally drop data packets instead of forwarding them are known as malicious nodes. They are introduced to the network to test and analyze the performance of the proposed model. The TCL (Tool Command Language) script depicted in below and shows various nodes that act as malicious in a network with 20 nodes (Box 1).

Box 1. Tool Command Language (TCL) script for malicious nodes.

```
Adding malicious nodes ot − at 0 "[node-(15) set ragent-] malicious"
Node 15 is set as malicious ot − at 0 "[node-(25) set ragent-] malicious"
Node 25 is set as malicious ot − at 0 "[node-(35) set ragent-] malicious"
Node 35 is set as malicious
```

Standard AODV is used as a reference to check whether the proposed protocol can efficiently mitigate against malicious attacks without compromising the performance.

4.3. Performance Metrics

This section discusses the performance metrics used to evaluate the performance of the proposed model.

4.4. Throughput

In computing, throughput is defined as the amount of data successfully transferred between a source and a sink over a given period (seconds). It can be computed as:

$$\mathrm{TP} = \frac{\text{Number of successfully received packets}}{\text{StopTime} - \text{StartTime}} \tag{10}$$

4.5. Routing Overhead

Routing overhead (RO) represents control packets that are required to perform a specific task. Thus, it is a sum of all the control packets sent during the total simulation time:

$$RO = \sum_{i}^{N} CP_i \tag{11}$$

Here, CP_i represents a number of control packets sent during each iteration i and N represents the total number of iterations.

4.6. Average End-to-End Delay

The average end-to-end delay is the average amount of time that packets take to travel from their source to their destination. It also includes the delay caused by re-transmission, buffering, and queuing. It can be computed as:

$$\text{EED} = \frac{1}{N\sum_{n=1}^{N}(r_n - s_n)} \quad \text{sec.} \tag{12}$$

Here, r_n shows the time when the packet is sent, s_n shows the time when a packet is received, and N shows the total number of packets received.

4.7. Packet-Delivery Ratio

The packet-delivery ratio is the ratio at which the data packets are successfully delivered to the destination. It can be computed as:

$$\text{PD} = \frac{\sum_{\forall i \in D} TPR_i}{\sum_{\forall i \in D} \times TPS_k} \times 100 \tag{13}$$

where TPR_i represents the total number of packets received by the DBR destination, i and TPS_k represent the total packets sent by the Constant Bit Rate (CBR) source k, and S denotes a collection of CBR sources. D represents a collection of CBR destinations.

5. Experimental Results and Comparative Analysis

The simulation results are evaluated extensively under varying network conditions, such as mobility, network size area, and node count. The performance metrics are obtained and analyzed when the proposed model is implemented by varying the number of nodes and mobility to prove that the proposed model can successfully implement energy-aware trust to provide secure communication via MANETs.

5.1. Performance Analysis

Figure 7 shows the end-to-end delay (in microseconds) analysis among the proposed and the existing Energy Efficient Partial Permutation Encryption (EEPPM) protocol [15]. It is found that the proposed model achieves lesser end-to-end delay values compared to EEPPM. The main reason behind this difference is that the proposed model can detect and remove the malicious nodes more efficiently than EEPPM.

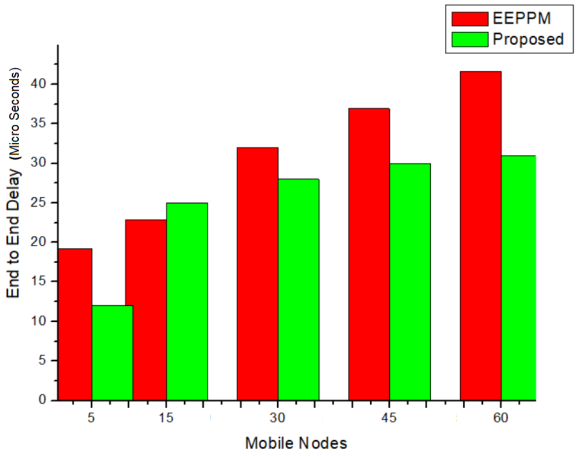

Figure 7. End-to-end delay analysis.

Figure 8 depicts the packet transformation ratio analysis between the proposed and existing EEPPM protocols. It is found that the proposed protocol achieves significantly bet-

ter packet-delivery ratio values than EEPPM. The proposed protocol outperforms EEPPM, in terms of packet-delivery ratio, by 2.8392%.

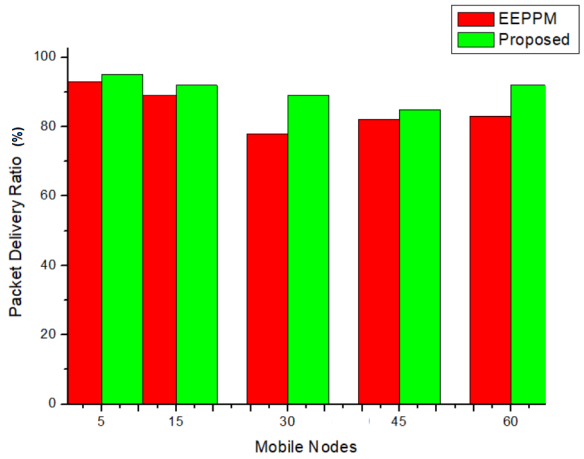

Figure 8. Packet-delivery analysis.

Figure 9 shows the throughput (unit packets/second) analysis between the proposed and EEPPM models. It is found that the proposed protocol achieves significantly better throughput performance values than EEPPM. The proposed protocol achieves 1.9258% better average throughputs than EEPPM.

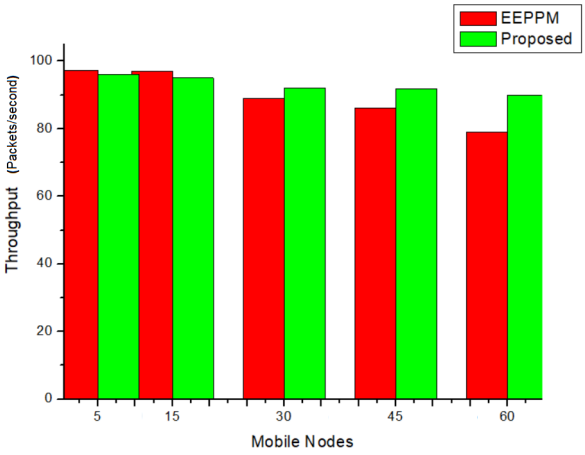

Figure 9. Throughput analysis.

Figure 10 depicts the percentage of communication overheads (the unit is communication overhead, and is shown in number of bits) analysis between the proposed and EEPPM protocols. The proposed model has a lesser percentage of communication overhead, whereas the EEPPM model has a higher percentage of communication overheads. In the proposed model, if any node is compromised, it will create security breaches. Here, if any node other than the CK and DK is compromised, there will be no effect on the security of the entire network. This will reduce overheads, but the existing model does not consider these factors. The proposed protocol achieves 3.1585% lesser communication overheads than EEPPM.

Figure 11 depicts the key (the unit is microseconds) computation time analysis between the proposed and EEPPM models. Key computation time refers to the time taken to perform the computation process. The proposed model takes less time for key computation, whereas the EEPPM model takes significantly more time for key computation. In the proposed model, all nodes need not compute their keys, as only the CK and DK nodes are responsible for it. This will reduce the key computation time, whereas, in case of the EEPPM model,

every node needs to compute its own keys. Due to the low computation capabilities of wireless nodes, the key computation time increases whenever the nodes are scaled to a higher value. The proposed protocol achieves a 2.6276% shorter key computation time than EEPPM.

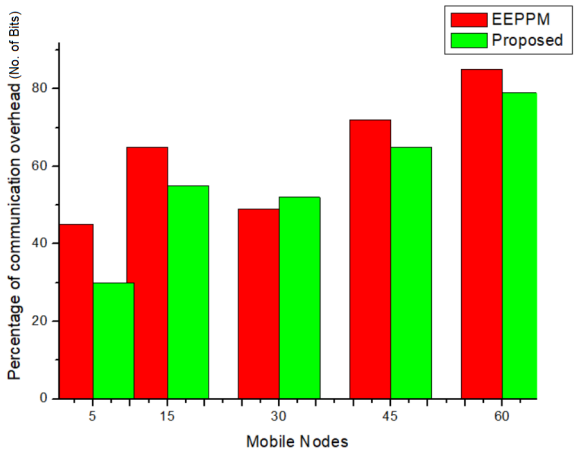

Figure 10. Percentage of communication overhead analysis.

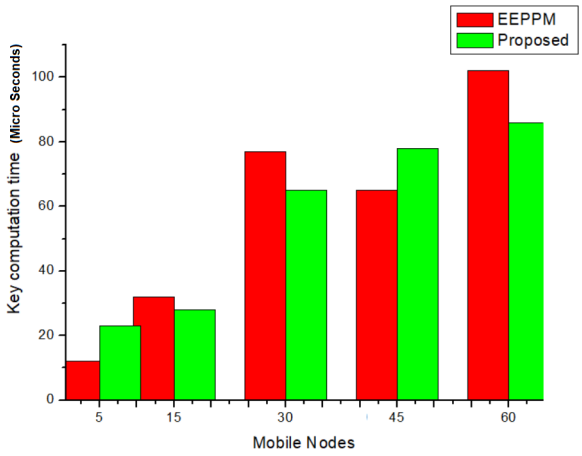

Figure 11. Key computation time analysis.

Figure 12 shows the energy consumption (watt-hour) analysis. The proposed model uses significantly less energy than the EEPPM model. In the proposed model, all nodes need not compute their keys; only the CK and DK nodes handle them. Thus, only two selected nodes consume energy during the key generation and distribution time, and this will improve the energy efficiency. Conversely, in the EEPPM model, every node needs to compute their own keys, resulting in more energy consumption. The proposed protocol outperforms EEPPM in terms of energy conservation by 1.3549%.

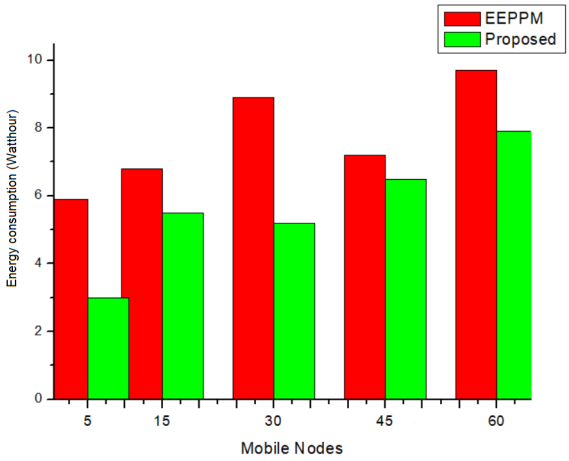

Figure 12. Energy consumption (watt-hour).

5.2. Comparative Analysis

Table 2 shows the comparative analysis among the proposed and the competitive routing protocols for MANETs. The selected competitive protocols are: ENACSC [13], ALARM [14], FACES [16], AMRP [17], STARS [18], and NSC [19]. The number of MANET nodes are set to 40. It is found that the proposed protocol achieves significantly better performance in terms of the average end-to-end delay (EED), packet-delivery ratio (PDR), throughput, and energy consumption. The major difference between the proposed and the competitive protocol is the use of the CK and DK nodes, which reduces the computation time of the MANET nodes significatly. Bold values indicate higher performance. The proposed protocol outperforms the competitive protocols in terms of EED, PDR, throughput, and energy consumption, by 2.4597%, 2.1578%, 2.6246%, and 3.6872%, respectively.

Table 2. Comparative analysis of the proposed model.

Protocol	EED	PDR	Throughput	Energy Consumption
ENACSC [13]	37.1317	81.8833	82.9983	6.6934
ALARM [14]	34.8151	84.6249	85.9999	6.2702
FACES [16]	39.3981	79.6719	81.0619	7.4092
AMRP [17]	38.8883	80.1767	81.5717	7.3336
STARS [18]	33.7127	85.5723	87.3473	6.1544
NSC [19]	39.8206	79.5294	80.6294	7.1802
Proposed	31.0567	87.9426	89.9438	5.5893

5.3. Future Scope

Further improvements of the proposed model can be achieved by using deep-learning models [41–43] to predict the CK and DK nodes efficiently. The effect of hyper-parameter tuning [44–46] is also ignored. Therefore, in the future, the hyper parameters of the proposed model will be optimized using various optimization approaches, such as genetic algorithms [47]. Additionally, in the future, the proposed model can be used for other kinds of wireless networks, such as Vehicular Ad Hoc Networks (VANETs).

6. Conclusions

From the review, it has been found that MANETs are prone to serious security threats that are difficult to resist using the existing security approaches. Therefore, various secure routing protocols were developed to strengthen the security of MANETs. In most of the existing routing protocols, every node is responsible for the generation and distribution of its own secret keys, which results in more energy dissemination. Moreover, if any node is compromised, security breaches should occur. To overcome these issues, a secure and

energy-efficient routing protocol was proposed by using group key management. Asymmetric key cryptography was used, which involves two specialized nodes: a Calculator Key (CK) and a Distribution Key (DK). These two nodes were responsible for the generation, verification, and distribution of secret keys. As a result, other nodes did not need to perform any kind of additional computation for building the secret keys. These nodes, i.e., the CK and DK, were selected using the energy consumption and trust values of nodes. Extensive experiments were performed by considering the existing and the proposed protocols. Performance analyses revealed that the proposed protocol outperforms the competitive protocols in terms of average end-to-end delay (EED), packet-delivery ratio (PDR), throughput, and energy consumption by 2.4597%, 2.1578%, 2.6246%, and 3.6872%, respectively.

Author Contributions: Conceptualization, P.B. and D.S.; Formal analysis, P.B. and D.S.; Funding acquisition, M.K. and H.-N.L.; Investigation and Methodology, P.B. and D.S.; Project administration, D.S.; Resources, M.K. and H.-N.L.; Software, Supervision, M.K. and H.-N.L.; Writing—original draft, P.B. and D.S.; Writing—review and editing, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported, in part, by the National Research Foundation of Korea (NRF) Grant, funded by the Korean government (MSIP) (NRF-2021R1A2B5B03002118). This research was also supported by the Ministry of Science and ICT (MSIT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-0-01835), supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ben Othman, J.; Mokdad, L. Enhancing data security in ad hoc networks based on multipath routing. *J. Parallel Distrib. Comput.* **2010**, *70*, 309–316. [CrossRef]
2. Kumar, K.V.; Jayasankar, T.; Eswaramoorthy, V.; Nivedhitha, V. SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks. *Int. J. Intell. Netw.* **2020**, *1*, 36–42. [CrossRef]
3. El-Hadidi, M.G.; Azer, M.A. Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs. In Proceedings of the 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 26–27 May 2021; pp. 155–160. [CrossRef]
4. Wu, W.C.; Liaw, H.T. A Study on High Secure and Efficient MANET Routing Scheme. *J. Sens.* **2015**, *2015*, e365863. [CrossRef]
5. Devi, V.S.; Hegde, N.P. Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer. *Wirel. Pers. Commun. Int. J.* **2018**, *100*, 923–940. [CrossRef]
6. Gomathy, V.; Padhy, N.; Samanta, D.; Sivaram, M.; Jain, V.; Amiri, I.S. Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 4995–5001. [CrossRef]
7. Kousar, R.; Alhaisoni, M.; Akhtar, S.A.; Shah, N.; Qamar, A.; Karim, A. A Secure Data Dissemination in a DHT-Based Routing Paradigm for Wireless Ad Hoc Network. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, e2740654. [CrossRef]
8. Maheswari, M.; Geetha, S.; Kumar, S.S.; Karuppiah, M.; Samanta, D.; Park, Y. PEVRM: Probabilistic Evolution Based Version Recommendation Model for Mobile Applications. *IEEE Access* **2021**, *9*, 20819–20827. [CrossRef]
9. Funderburg, L.E.; Lee, I.Y. A Privacy-Preserving Key Management Scheme with Support for Sybil Attack Detection in VANETs. *Sensors* **2021**, *21*, 1063. [CrossRef] [PubMed]
10. Perkins, C.E.; Bhagwat, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Comput. Commun. Rev.* **1994**, *24*, 234–244. [CrossRef]
11. Perkins, C. Ad Hoc on Demand Distance Vector (aodv) Routing Ietf. Internet Draft, draft-ietf-manet-aodv-00.txt. 1997. Available online: https://datatracker.ietf.org/doc/rfc3561/ (accessed on 16 January 2021).
12. Broch, J.; Johnson, D.B.; Maltz, D.A. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. draft-ietfmanet-dsr-03. txt. Work-in-Progress. 1998. Available online: https://www.ietf.org/proceedings/42/I-D/draft-ietf-manet-dsr-00.txt (accessed on 16 January 2021).
13. Saxena, N.; Tsudik, G.; Yi, J.H. Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *20*, 158–170. [CrossRef]

14. El Defrawy, K.; Tsudik, G. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. *IEEE Trans. Mob. Comput.* **2011**, *10*, 1345–1358. [CrossRef]
15. Khan, A.; Sun, Q.T.; Mahmood, Z.; Ghafoor, A.U. Energy efficient partial permutation encryption on network coded MANETs. *J. Electr. Comput. Eng.* **2017**, *2017*, 4657831. [CrossRef]
16. Dhurandher, S.K.; Obaidat, M.S.; Verma, K.; Gupta, P.; Dhurandher, P. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems. *IEEE Syst. J.* **2011**, *5*, 176–188. [CrossRef]
17. Chen, S.; Wu, M. Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. *J. Syst. Eng. Electron.* **2011**, *22*, 519–527. [CrossRef]
18. Qin, Y.; Huang, D.; Li, B. STARS: A Statistical Traffic Pattern Discovery System for MANETs. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 181–192. [CrossRef]
19. Saxena, N.; Yi, J.H. Noninteractive Self-Certification for Long-Lived Mobile Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 946–955. [CrossRef]
20. Hammamouche, A.; Omar, M.; Djebari, N.; Tari, A. Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. *J. Inf. Secur. Appl.* **2018**, *43*, 12–20. [CrossRef]
21. Subramaniyan, S.; Johnson, W.; Subramaniyan, K. A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 205. [CrossRef]
22. Veeraiah, N.; Ibrahim Khalaf, O.; Prasad, C.V.P.R.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S.A.; Alsufyani, N. Trust Aware Secure Energy Efficient Hybrid Protocol for MANET. *IEEE Access* **2021**, *9*, 120996–121005. [CrossRef]
23. Srilakshmi, U.; Veeraiah, N.; Alotaibi, Y.; Alghamdi, S.A.; Khalaf, O.I.; Subbayamma, B.V. An Improved Hybrid Secure Multipath Routing Protocol for MANET. *IEEE Access* **2021**, *9*, 163043–163053. [CrossRef]
24. Elhoseny, M.; Shankar, K. Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique. *IEEE Trans. Reliab.* **2020**, *69*, 1077–1086. [CrossRef]
25. Sankaran, K.S.; Vasudevan, N.; Devabalaji, K.R.; Babu, T.S.; Alhelou, H.H.; Yuvaraj, T. A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks. *IEEE Access* **2021**, *9*, 21735–21745. [CrossRef]
26. Malathi, M.; Jayashri, S. Modified Bi-directional Routing with Best Afford Path (MBRBAP) for Routing Optimization in MANET. *Wirel. Pers. Commun.* **2016**, *90*, 861–873. [CrossRef]
27. Aftab, F.; Zhang, Z.; Ahmad, A. Self-Organization Based Clustering in MANETs Using Zone Based Group Mobility. *IEEE Access* **2017**, *5*, 27464–27476. [CrossRef]
28. Kaur, M.; Singh, D.; Kumar, V.; Gupta, B.B.; Abd El-Latif, A.A. Secure and Energy Efficient-Based E-Health Care Framework for Green Internet of Things. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1223–1231. [CrossRef]
29. Zhang, T.; Zhao, S.; Cheng, B.; Farina, M.; Huang, J.; Chen, J.; Ren, B.; Hou, S. Lightweight SOA-Based Multi-Engine Architecture for Workflow Systems in Mobile Ad Hoc Networks. *IEEE Acess* **2018**, *6*, 14212–14222. [CrossRef]
30. Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. A survey of routing attacks in mobile ad hoc networks. *IEEE Wirel. Commun.* **2007**, *14*, 85–91. [CrossRef]
31. Singh, T.; Saxena, N.; Khurana, M.; Singh, D.; Abdalla, M.; Alshazly, H. Data Clustering Using Moth-Flame Optimization Algorithm. *Sensors* **2021**, *21*, 4086. [CrossRef]
32. Chauhan, K.K.; Sanger, A.K.S. Key Management for Group Based Mobile Ad Hoc Networks. In *International Conference on Computer Science and Information Technology*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 455–464._46. [CrossRef]
33. Shibu, K.R.; Suji Pramila, R. Load Based Key Generation for MANETs: A Comparative Study with DSR and AODV. *Wirel. Pers. Commun.* **2021**, *116*, 1703–1712. [CrossRef]
34. Singh, A.; Maheshwari, M.; Nikhil; Kumar, N. Security and Trust Management in MANET. In *International Conference on Advances in Information Technology and Mobile Communication*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 384–387. [CrossRef]
35. Pamarthi, S.; Narmadha, R. Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications. *Wirel. Pers. Commun.* **2021**. [CrossRef]
36. Zhang, T.; Xu, X.; Zhou, L.; Jiang, X.; Loo, J. Cache Space Efficient Caching Scheme for Content-Centric Mobile Ad Hoc Networks. *IEEE Syst. J.* **2019**, *13*, 530–541. [CrossRef]
37. Zhang, D.G.; Zhao, P.Z.; Cui, Y.Y.; Chen, L.; Zhang, T.; Wu, H. A New Method of Mobile Ad Hoc Network Routing Based on Greed Forwarding Improvement Strategy. *IEEE Access* **2019**, *7*, 158514–158524. [CrossRef]
38. Xu, H.; Zhao, Y.; Zhang, L.; Wang, J. A Bio-Inspired Gateway Selection Scheme for Hybrid Mobile Ad Hoc Networks. *IEEE Access* **2019**, *7*, 61997–62010. [CrossRef]
39. Dbouk, T.; Mourad, A.; Otrok, H.; Tout, H.; Talhi, C. A Novel Ad-Hoc Mobile Edge Cloud Offering Security Services Through Intelligent Resource-Aware Offloading. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 1665–1680. [CrossRef]
40. Bettstetter, C.; Hartenstein, H.; Pérez-Costa, X. Stochastic properties of the random waypoint mobility model. *Wirel. Netw.* **2004**, *10*, 555–567. [CrossRef]
41. Gupta, B.; Tiwari, M.; Lamba, S.S. Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement. *CAAI Trans. Intell. Technol.* **2019**, *4*, 73–79. [CrossRef]
42. Hu, G.; Chen, S.H.K.; Mazur, N. Deep Neural Network-based Speaker-Aware Information Logging for Augmentative and Alternative Communication. *J. Artif. Intell. Technol.* **2021**, *1*, 138–143.

43. Ghosh, S.; Shivakumara, P.; Roy, P.; Pal, U.; Lu, T. Graphology based handwritten character analysis for human behaviour identification. *CAAI Trans. Intell. Technol.* **2020**, *5*, 55–65. [CrossRef]
44. Jiang, D.; Hu, G.; Qi, G.; Mazur, N. A fully convolutional neural network-based regression approach for effective chemical composition analysis using near-infrared spectroscopy in cloud. *J. Artif. Intell. Technol.* **2021**, *1*, 74–82. [CrossRef]
45. Xu, Y.; Qiu, T.T. Human Activity Recognition and Embedded Application Based on Convolutional Neural Network. *J. Artif. Intell. Technol.* **2021**, *1*, 51–60. [CrossRef]
46. Basavegowda, H.S.; Dagnew, G. Deep learning approach for microarray cancer data classification. *CAAI Trans. Intell. Technol.* **2020**, *5*, 22–33. [CrossRef]
47. Kaur, M.; Kumar, V.; Yadav, V.; Singh, D.; Kumar, N.; Das, N.N. Metaheuristic-based deep COVID-19 screening model from chest X-ray images. *J. Healthc. Eng.* **2021**, *2021*, 8829829. [CrossRef] [PubMed]