sustainability

MDPI

Article

Efficient Neighbour Feedback Based Trusted Multi Authenticated Node Routing Model for Secure Data Transmission

Praveen Bondada [1], Debabrata Samanta [1,2], Shehzad Ashraf Chaudhry [3] , Yousaf Bin Zikria [4,*] and Farruh Ishmanov [5,*]

[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 (Deemed to be) University, Bangalore 560029, India
[3] Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul 34310, Turkey; sashraf@gelisim.edu.tr
[4] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea
[5] Department of Electronics and Communication Engineering, Kwangwoon University, Seoul 01897, Korea
* Correspondence: yousafbinzikria@ynu.ac.kr (Y.B.Z.); farruh@kw.ac.kr (F.I.)

Abstract: The Mobile Ad Hoc Network (MANET) is a network that does not have a fixed infrastructure. Migratory routes and related hosts that are connected via wireless networks self-configure it. Routers and hosts are free to wander, and nodes can change the topology fast and unexpectedly. In emergencies, such as natural/human disasters, armed conflicts, and emergencies, the lowest configuration will ensure ad hoc network applicability. Due to the rapidly rising cellular service requirements and deployment demands, mobile ad-hoc networks have been established in numerous places in recent decades. These applications include topics such as environmental surveillance and others. The underlying routing protocol in a given context has a significant impact on the ad hoc network deployment power. To satisfy the needs of the service level and efficiently meet the deployment requirements, developing a practical and secure MANET routing protocol is a critical task. However, owing to the intrinsic characteristics of ad hoc networks, such as frequent topology changes, open wireless media and limited resources, developing a safe routing protocol is difficult. Therefore, it is vital to develop stable and dependable routing protocols for MANET to provide a better packet delivery relationship, fewer delays, and lower overheads. Because the stability of nodes along this trail is variable, the route discovered cannot be trusted. This paper proposes an efficient Neighbour Feedback-based Trusted Multi Authenticated Node (NFbTMAN) Routing Model. The proposed model is compared to traditional models, and the findings reveal that the proposed model is superior in terms of data security.

Keywords: mobile ad hoc network; MANET; authenticated routing mode; neighbour feedback

Citation: Bondada, P.; Samanta, D.; Chaudhry, S.A.; Zikria, Y.B.; Ishmanov, F. Efficient Neighbour Feedback Based Trusted Multi Authenticated Node Routing Model for Secure Data Transmission. *Sustainability* **2021**, *13*, 13296. https://doi.org/10.3390/su132313296

Academic Editors: Chien-Ming Chen, Marko Hölbl, SK Hafizul Islam and Marimuthu Karuppiah

Received: 10 October 2021
Accepted: 26 November 2021
Published: 1 December 2021

1. Introduction

Wireless networks involve different nodes corresponding via a wireless path. Few networks are connected to Wi-Fi only with the last hop. Examples include mobile voice, data, and mobile IP networks. In the last half, a decade, Desktop Computers have changed to networked agents who rely primarily on connectivity from independent workstations [1]. Email, cloud storage, and the international web are some of the specific educational and corporate services supplied. In addition, mobile device, tablet, and notebook computing is expanding every year [2].

In recent decades, research has been conducted on mobile ad-hoc networks due to the large availability of wireless communication services and fast growing need for deployment [3–5]. A MANET is an ongoing, self-configured mobile device network

connected wirelessly by the infrastructure. MANETs are characterised by mobility, self-government, hurried exploitation, and low-cost facilities that make it possible for them to be deployed for different purposes, such as observing the environment, adversity assistance, and military communication. One key benefit of a decentralised network is that, because of the multi-hop style of data transmission, they are often more robust than centralised networks [6].

For instance, the coverage decreases when a base station stops working in the cellular network configuration. The possibility of a single failure point in a MANET is significantly decreased because the data can traverse in several paths. Since MANET design develops over time, it has the ability to overcome problems such as network isolation or disconnection [7]. Proper routing is critical to the desired service supply as well as better communication and security in such a collaborating communications environment [8,9]. However, MANET is faced with additional safety and performance issues with the dynamic network topology, the usage of open wireless media, and constrained resource limitations. Therefore, MANET has been very interested in inventing an efficient and secure routing protocol in the research community. The MANET structure is depicted in Figure 1.

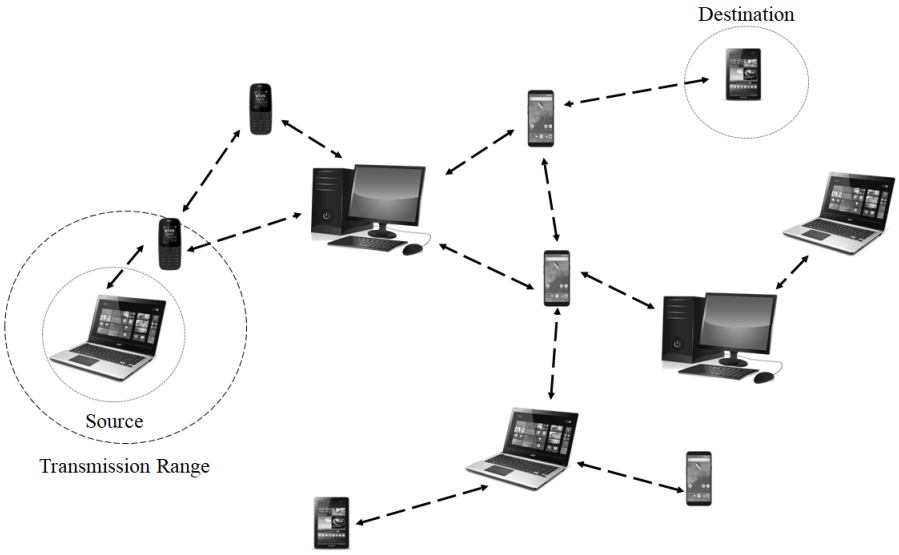

Figure 1. MANET Structure.

Different safe routing methods were developed throughout the years to protect WSNs against malicious and selfish behaviour. These routing protocols depend, however, principally on basic versions and authentication procedures. Most cryptographic algorithms require significant computational capability and energy consumption, in particular the asymmetrically encrypted procedure. The low cost sensor nodes, however, are generally resource-limited in memory, energy, and computer capabilities [10]. Several authentications and encryption schemes in routing protocols need a central authority or centralised management, which in WSNs is frequently unworkable. Finally, adversaries may hack the sensor nodes in an intentioned area by physical means. All safety systems can become useless once the keys are released. In other words, standard safe cryptographic-based protocols can withstand some sorts of external attacks but do not guard against inside nodes bad behaviour.

MANET exchanges nodes or mobile node groups for a large number in a safety-critical environment with data and control messages. These messages must be adapted to the deployment scenario, time, and geographical area. In addition, in the presence of environmental limits, compliance with different performance measurements, different degrees of safety requirements, and robustness must be ensured [11,12]. Violations of security and performance may lead to major consequences, for example, erroneous information or delayed transmission of crucial communications. The main cause is serious damage to the

assets of the nation. Inefficient and unsafe routing of ad hoc nodes may lead deliberately in MANET to evaluation-safety concerns [12]. The rest of the study is structured as follows: An overview of the existing routing protocols for MANETs is given in Section 2, followed by the literature survey in Section 3. The proposed model is explained in Section 4. The results are given in Section 5 and the study is concluded in Section 6.

2. Routing Protocol Types

In MANET, there are different routing mechanisms. Three sorts of routing systems are available: proactive, reactive, and hybrid. The MANET routing methods are used for dealing with a considerable number of limited-resource nodes. The true concern in routing is the entry/departure of the network nodes [13,14]. Despite the development of several mobile nodes, it is vital to reduce the overhead routing message. The measurement of the routing table is another critical concern. The extent of the routing technique is more significant than the control packets that are transmitted inside the system can affect. The routing procedure determines the optimal route to the destination and how and when courses are determined. Figure 2 demonstrates the case of the kind of routing method.

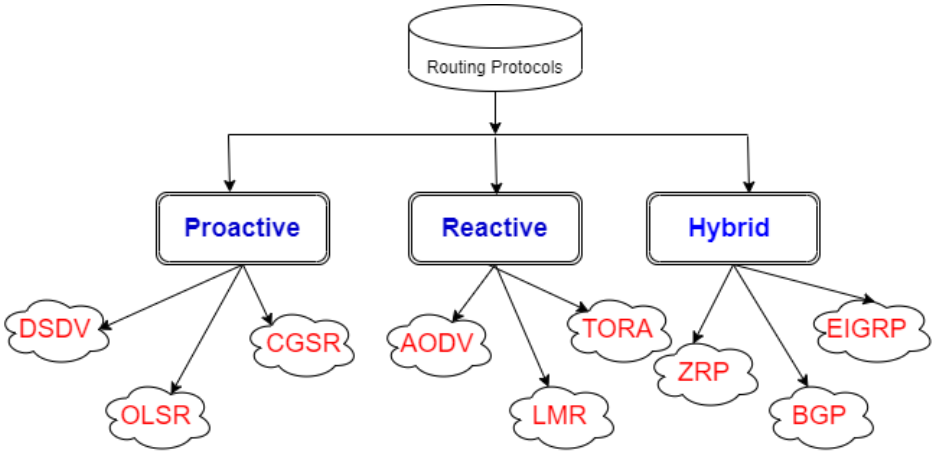

Figure 2. Routing Protocols.

A trust-based multi-authenticated routing protocol is a protocol in which a node considers a routing decision based on the behaviour of a candidate router and its validation status. This view is quantified and referred to as the Trusted Validation metric. The route from source to destination is determined based on trust metrics [15]. Trust based routing is vital to ensure the information collected, to preserve network performance against inappropriate consumption and network resources. Most uses of WSN convey and provide very vital information and secrecy, such as for military and health purposes [16]. WSN infected with misbehaving nodes is misrouting traffic to misrepresentation or is not transmitting packets towards the destination that cause information loss. A trustworthy protocol on routing can protect the interchange of data, provide safety information, and protect the value of the data. However, the classic routing methods based on trust have certain essential limitations [17]. The trust based systems deal with threats inherent in wireless networks and also create additional hazards that need to be paid particular attention [18]. In this manuscript, a trust based multi authenticated routing model is proposed to deal with the problems mentioned earlier. The routing algorithm in our system considers the characteristics of the trust measure and other path selection quality requirements.

3. Literature Survey

The Dynamic Learning System proposed by Muthusenthil et al. [19] guarantees the number of sequences on the routing table of the node receiving the route reply packet. The packet is deleted or allowed if it is larger than in the route reply packet. The value of the sequence number should not exceed or be classified as an attacker node. Dynamically

this value of the threshold varies. The simulation results demonstrate that the time limit is reduced, but the routing overhead is increased.

The method designed by Anand et al. [20], based on the neighbourhood and the protocol on the rehabilitation route, has two phases: detection and response. To detect the first gathering of the information from the neighbour node, packets are analysed. This is done with the packet, which is unicast by the source node following receipt of the ack message. Destination D Secondly, the source compares the next set of information after receiving more than one message. If the difference exceeds the threshold, a node of the black hole is found [16]. S delivers the MRE (Modified Route Entrance) packet to the destination after discovering the true destination. As a result, the output is raised; false positive probabilities and overhead routing are reduced.

Venkanna et al. [21] have presented an agent based multi-cast routing scheme (ABMRS) in MANETs using mobile/static unit collecting. The new technique progresses accordingly: (1) Reliables nodes have been found; (2) intermediate nodes have been connected to reliable and intermediate nodes; (3) multicast backbones have been established; and (4) multi-cast groups members have been combined to backbones.

Malathi et al. [22] offered the comparison between AODV, OLSR and HWMP in their study "energy and performance assessment of reactive, proactive and hybrid routing algorithms in the network wireless mesh." They employed an NS3 simulator and the following measures: power consumption, transmission, *PDR*, delay, e-transmission and e-PDR. The routing protocols were assessed using two topologies: grid topology and topology for mobile nodes. The results show that OLSR is the most effective in *PDR* and reduced delay routing technique. However, mobility and scalability can greatly affect its performance [23,24].

In order to identify and safeguard the selfish nodes for network security improvement, Devi et al. [25] developed the dynamic trust-based intrusion detection technique. The AODV was used here to generate the path from the source to the destination. Through the direct and indirect levels of trust, the selfish nodes were validly identified. Additionally, the direct and indirect trust degrees were analysed via neighbour's direct communication exchanges and recommendations. Overhead was introduced during data transfer by the frequent network topology.

A protocol to secure On-Demand routing protocols that use broadcasting as their route query mechanism is the Secure Routing Protocol (SRP) created by Hammamouche et al. [26]. They pointed out that a number of existing reactive routing protocols, notably the DSR, can be extended. Between a source node and a destination node, a security association (SA) is necessary. The SA will be defined by a common key between the two nodes. The SA is presumed [27,28].

The Ad-Hoc routing Security-aware (SAR) protocol is an ad-hoc routing solution that integrates security features as route discovery parameters. However, typical unprotected routing protocols identify the shortest way between two nodes, but SAR can identify a path with security features. For example, when each node on the route needs a particular shared key, the criterion for a valid route can be detected.

Authenticated Ad hoc Networks Routing (ARAN), as defined by Hammamouche et al. [29], is a secure on-demand routing protocol. ARAN uses an encryption mechanism to provide authentication, message integrity, and non-repudiation security objectives. The first phase is the exploratory certification process requiring a trustworthy certificate authority. It consists of two different operating phases. All nodes wishing to connect to the network must contact the certifying body and ask for an address and a public key certificate. The certifying body gives its public key to all network nodes [30,31]. The second stage in the protocol's operation is the route finding process, which supplies final authentication. This guarantees that the destination is reached.

4. Proposed Model

An autonomous framework consisting of separate nodes that can move about in its own direction is called MANET. This framework might be used as stand-alone, or could connect to a pre-existing system. The mobility nature of MANET makes the topology dynamic [32]. It is possible for the source and destination to validly transfer data if they are either both inside the transmission range or if they are using transferring nodes that connect two of them. Other than being wired, MANETs have a few distinct features. The first point to consider is that MANETs utilise dynamic connections to transmit packets. Their susceptibility characterises wire-line connections to time and space; they may also be obstructed by reflection, refraction, diffraction, and distortion. Restricted data transfer capacity is another disadvantage of remote paths [33,34]. In MANETs, the topology can alter radically, and problems in routing can occur, whereas, in wired systems, the topology remains constant. as a result, in MANETs, conventions must adjust to avoid routing failures.

Because MANETs vary so much, components designed for wired systems cannot be properly mapped to MANETs. Quality of Service (QoS) arrangement in MANETs is made up of activities at different tiers, such as network and application layers, in which the network layer is given the primary role. In the network layer, the routing convention must be able to accommodate QoS requirements for the beginning of a session and respond to portability issues. A routing protocol should decide when many paths are available, and a secure path needs to be recognised to transmit data packets. When only certain paths are used, the performance of a routing protocol should always be the same as the shortest path routing protocol [32,35]. In the proposed model, neighbour feedback is considered by every node for availing the trust on the nodes, and only nodes with positive feedback are considered. Then every node undergoes multi-authentication to avoid malicious actions in the network. Initially, the node will be authenticated by the neighbour node. If the node exhibits any malicious operations, the node will not be authenticated and removed from the routing process. After successful authentication of the neighbour node, the node will be authenticated by the Network Head Node (*NHN*), which is the node that monitors all the nodes and their behaviours during data transmission. Network Head Node (*NHN*) consists of an organisational network that connects the cluster's head node and other nodes in some cases. Most users connect to the workplace network via the public or organisation network to do their work. Unless a private network and, optionally, an application network connect the cluster nodes, all intra-cluster administration and deployment traffic is transmitted on the enterprise network. The proves of routing and using *NHN* node is depicted in the Figure 3.

Each node will be authenticated by its neighbour node and then by NHN node in the figure. Multi-level authentication is performed, and also neighbour feedback is considered for establishing a strong and secure route for secure data transmission. Initially, during a dummy data transmission, the packet delivery rate, computational capability rate, packet loss rate, energy consumption, the behaviour of every node is calculated. A node with a high packet delivery rate, less energy consumption, and high computational capabilities is selected as NHN node. The route identifier serves as the foundation for effective urban traffic planning and simulation. Each route within a feature class is given a unique ID. Any integer or character field in your route feature class can be used as the route identifier.

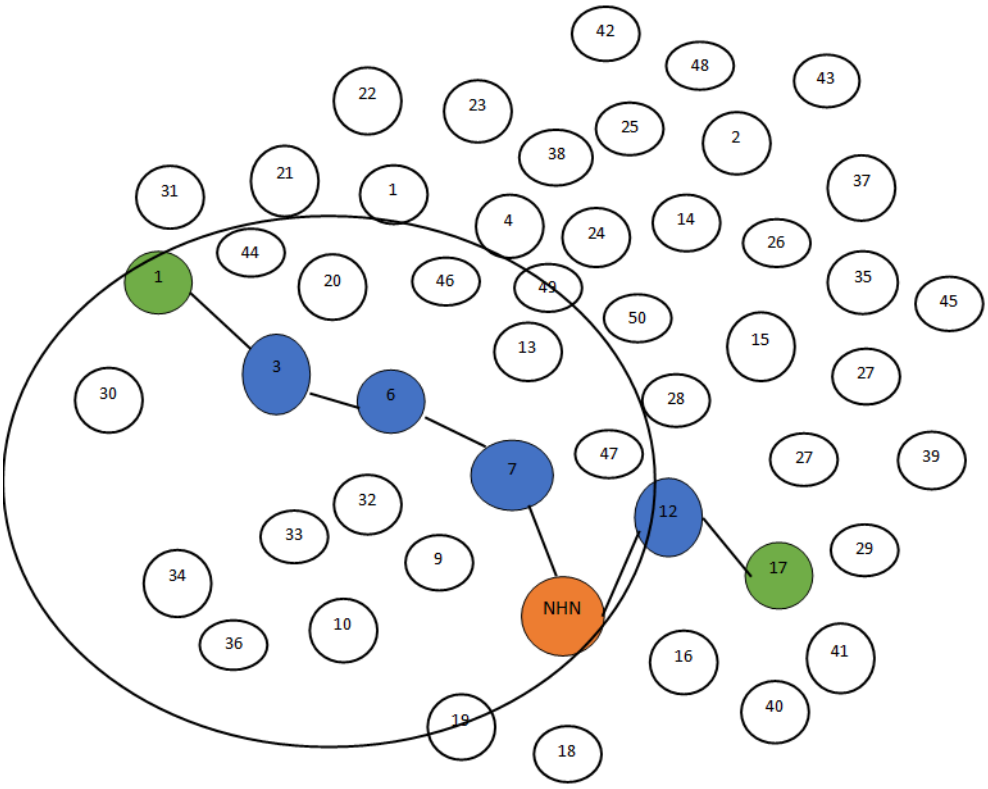

Figure 3. Routing Process in Network.

We consider coordinates $Ni(Xi, Yi)$ for each node with its node ID (NID) to NHN node. The NHN node will broadcast the Route Identification Token (RIT) to all the nodes considered to be involved in data communication. The Nodes after receiving the RIT message, will get their neighbour IDs and transmit to NHN node as:

$$array(NHN) = \sum_{i \in N_l} \sum_{i,j} \frac{NID^i}{DID^j} + mintime[N(i)]_j^l + Z \tag{1}$$

$$Z = neighbour[NID]_j^i. \tag{2}$$

The distance between the node $n(i)$ and neighbour node is calculated as:

$$\text{Min}(N(i), N(i+1)) = \sqrt{P + Q} \tag{3}$$

$$P = \left(X_{N(i+1)(t)} - X_{N(i)(t)}\right)^2 \tag{4}$$

$$Q = \left(Y_{N(i+1)(t)} - Y_{N(i)(t)}\right)^2. \tag{5}$$

The neighbour node $N(i+1)$ will send the feedback about the node $N(i)$ to the NHN node as:

$$Feedback[NID(i)] = \sum_{i=0, j=i+1}^{N} \frac{W}{totalnodes} \tag{6}$$

$$W = PDR(N(i)) + \sum_{i=0, j=i+1}^{N} eneglevel[N(i)_{(i,j)}] + U \tag{7}$$

$$U = min(Xi, Yi). \tag{8}$$

Here, PDR is the packet delivery rate, $min(Xi, Yi)$ is the neighbour node at nearest position. Based on the calculated neighbour feedback, the neighbour node will authenticate the node $N(i)$ and mark with label. The Feedback$(NID(i) > Th)$, so all Nodes will be authenticated and labelled as $SID++$ and update this to NHN node. The node that is authenticated will send the label to the NHN node. The NHN node will verify and again authenticate with an extra label calculated as:

$$NHNlabel[N(i)] = SID + DID * label(N(i)). \tag{9}$$

The NHN node calculates every node's mobility speed 'S' to calculate a new route if any failure occurs. The node speed is calculated as:

$$S[N(i)] = \frac{|(X_2 - X_1) + (Y_2 - Y_1)|}{(t + \Delta t) - t}, \tag{10}$$

where $S[N(i)]$ is the speed of a node, and t is the time instance and is the change in the time in T seconds, where T is the threshold time. The process of route identification is performed using Algorithm 1.

Algorithm 1: Route Identification

Input: Total node count, node, Source ID, Destination ID
initialization;
Step 1:Perform node labelling.
Step 2: Initialise node deployment for each node.
Step 3: Broadcast node position Co-ordinates to network.
Step 4: When a network is established, every node will send its node ID Source to Destination node.
Step 5: The Destination node will broad cast the Route Identification Token to all the nodes which are considered to involve in data communication.
Step 6: The Nodes after receiving the RIT message will get its neighbour IDs and transmit to Destination node.
Step 7: The Destination node will analyse the neighbour IDs and finalise the route and update it in the routing table.
Step 8: The distance between the node and neighbour node is calculated and store in table.
Step 9: The neighbour node will send the feedback about the previous node to the Destination node.
Step 10: Based on the calculated neighbour feedback, the neighbour node will authenticate the node and mark with label.Node will be authenticated and labelled.
Else
Node will be discarded from the route and go to step 5;
Step 11: The node which is authenticated will send the label to the Destination node. The Destination node will verify and again authenticate with extra label calculated.
Step 12: The node which is authenticated in multiple levels are updated in the routing table and then the Destination node will initiate the data transmission.
Step 13: The node mobility speed of every node is calculated by the Destination node to calculate a new route if any failure occurs.

5. Results

Due to features such as changeable topology and openness, MANET is vulnerable to many attacks. This leads to the exploitation of MANET in the presence of malevolent, or selfish nodes through many forms of assaults. Such nodes affect MANET routing performance, such as the delivery ratio of packets. The need for a factor of trust between nodes of communication is therefore justified in this proposed model. The proposed model is implemented in the NS2 simulator that establishes a MANET, and routing is performed on trusted nodes by considering the neighbour feedback. Every node undergoes multi authentication to strictly avoid malicious nodes so that the network's performance will be increased. The proposed Neighbour Feedback-based Trusted Multi Authenticated Node (NFbTMAN) Routing Model is compared with the Novel Energy Efficient Trust Aware

Routing (NETAR) model. The proposed model considers parameters such as Trust Factor Generation Time Levels, Route Identification Time Levels, Neighbour Feedback Assessment Level, Multi-Authentication Timed Levels, Packet Delivery Rate. The parameters considered for network formation are depicted in Table 1.

Network trust evaluation is utilised to promote secure and trustworthy networking by helping nodes collaborate in a trustworthy manner. However, there are still many difficulties and flaws with many trust management models proposed for the MANET. The proposed model trust factor generation time levels are compared with the traditional model, and the results are depicted in the Figure 4. Table 2 represents trust factor generation time levels.

Table 1. Simulation Parameters.

Parameter	Value
Number of simulated Nodes	20-40-60-80-100 nodes
Area size of topography (m)	500 m × 500 m
Radio range	150 m
Packet size	1000 byte
Send rate of traffic	4 packets/s
Traffic type	cbr
Number of traffic sources	4
Pause Time (s) at simulation	lOs
Simulation Time	80 s
Simulated Routing Protocols	AODV

Table 2. Trust Factor Generation Time Levels.

Network Nodes	Trust Factor Generation Time Levels	
	NFbTMAN Model	NETAR Model
10	20	20
20	28	30
30	30	38
40	34	42
50	40	50
60	40	58
70	45	61
80	50	75
90	52	88

Changes in route topology occur because of node mobility and, because of this, the system's architecture remains unforeseen for some time. Due to the decentralised nature of such networks, network communications must identify routes with high security. In the route discovery phase, the trust calculation is performed to include trusted nodes. The proposed model route identification time levels are compared with the traditional model, and the results are indicated in Figure 5. Route identification time levels are shown in Table 3.

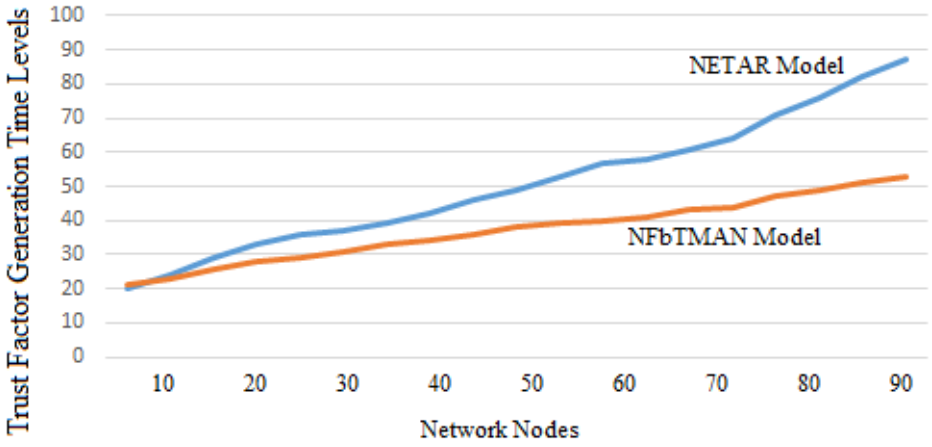

Figure 4. Trust Factor Generation Time Levels.

Table 3. Route Identification Time Levels.

Network Nodes	Route Identification Time Levels	
	NFbTMAN Model	NETAR Model
10	8	32
20	14	38
30	18	42
40	22	48
50	28	53
60	32	57
70	40	60
80	43	65
90	50	75

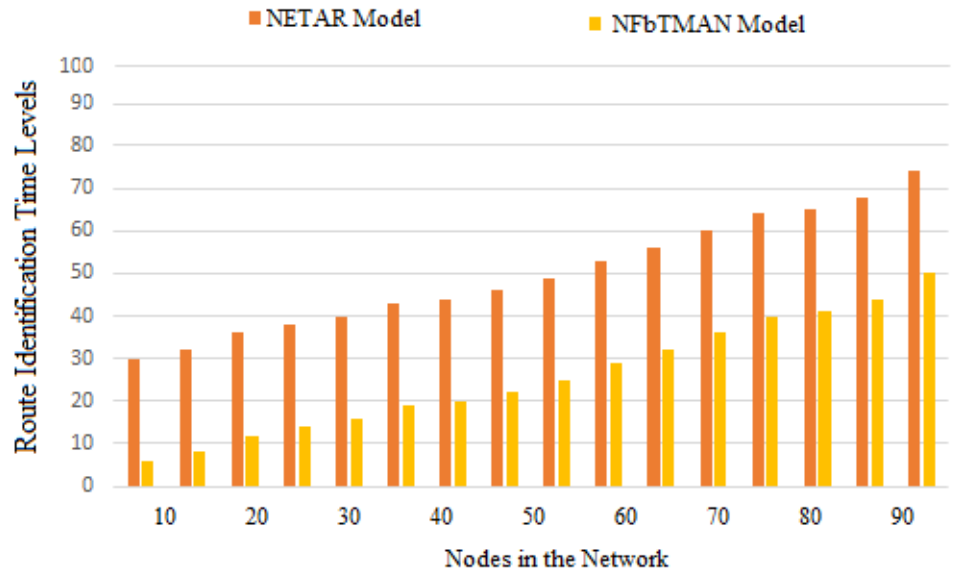

Figure 5. Route Identification Time Levels.

The proposed model considers neighbour feedback to establish a route, and the feedback assessment levels are represented in Figure 6. The feedback will help analyse the

node behaviour for considering only trusted nodes in finalising the route for secure data transmission. Table 4 express neighbour feedback assessment time level.

Table 4. Neighbour Feedback Assessment Time Level.

Network Nodes	Neighbour Feedback Assessment Time Level	
	NFbTMAN Model	NETAR Model
10	20	50
20	25	60
30	30	70
40	38	75
50	40	79
60	45	80
70	50	85
80	58	90
90	60	95

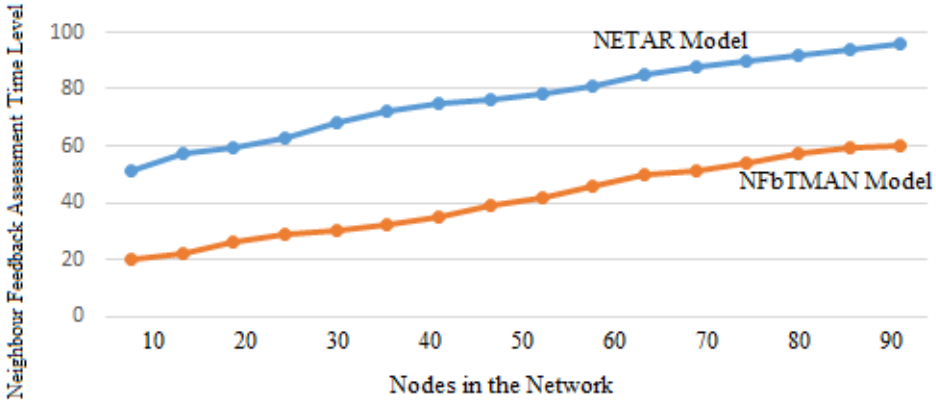

Figure 6. Neighbour Feedback Assessment Time Level.

It is possible for MANETs to be targeted by numerous attacks. Eavesdropping, interference, impersonation, and denial of service are all possible techniques. Redundant transmission and robust authentication can be utilised to increase the security of a MANET. They are capable of handling only a fraction of the threat. The multi authentication time levels of the proposed and traditional models are indicated in Figure 7. Table 5 shows multi-authentication time levels.

The packet delivery rate is defined as the ratio of the number of packets transmitted by the source node to the number of packets received by the destination node. A route with trusted nodes is considered in the proposed paradigm. When compared to the traditional model, the proposed model has a high packet delivery rate. The packet delivery rates of the traditional and proposed models are depicted in Figure 8. Table 6 shows packet delivery rate.

Table 5. Multi-Authentication Time Levels.

Network Nodes	Multi Authentication Time levels	
	NFbTMAN Model	NETAR Model
10	18	45
20	22	60
30	25	62
40	30	65
50	35	70
60	38	75
70	40	82
80	40	95
90	42	98

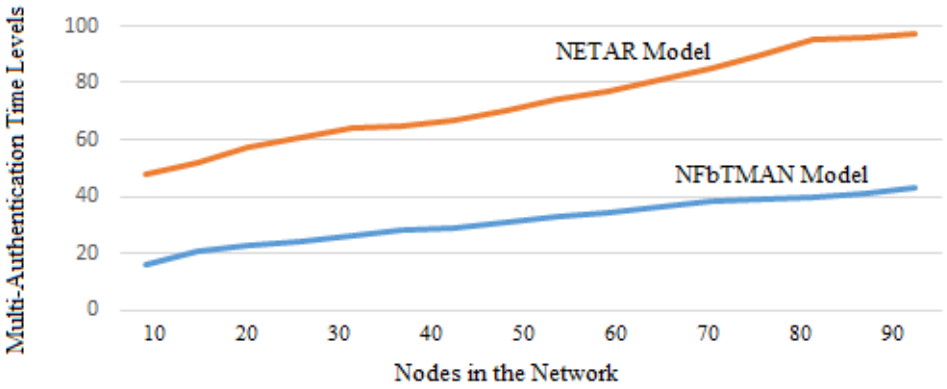

Figure 7. Multi-Authentication Time Levels.

Table 6. Packet Delivery Rate.

Network Nodes	Packet Delivery Rate	
	NFbTMAN Model	NETAR Model
10	55	15
20	60	20
30	65	22
40	70	25
50	75	30
60	80	35
70	85	40
80	90	50
90	95	55

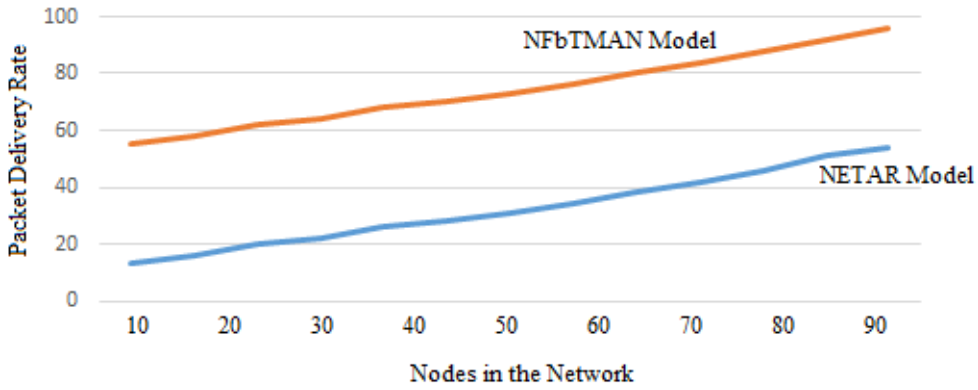

Figure 8. Packet Delivery Rate.

6. Conclusions

MANET is a group of mobile nodes that can dynamically transfer positions in another network to share information. Mobility causes linkages to break down, lengthening the time it takes to retrace one's steps. This study proposes a MANET routing algorithm that overcomes the constraints of existing routing protocols. The suggested routing strategy, in contrast to earlier work, uses node speed, direction, and residual energy to generate more stable routes between intermediate nodes in the source and destination node paths. Through extensive simulations, it has demonstrated that the approaches presented are effective in a variety of operational situations and scenarios. To construct a secure data transmission path, the suggested model takes into account the trust factor and neighbour feedback, as well as multi-level authentication. The suggested approach effectively determines the secure path by analysing authenticated nodes in order to avoid malicious network behaviours. The proposed model has a high packet delivery ratio, and the latency is decreased. When compared to typical models, the presented model has an extremely low packet loss rate. The multi-level authentication and trust factor computation processes can be modified in the future to decrease node overhead and increase performance.

Author Contributions: Conceptualization, P.B. and D.S.; Formal analysis, P.B. and D.S.; Funding acquisition, D.S. and Y.B.Z.; Investigation, S.A.C. and F.I.; Methodology, P.B., S.A.C., Y.B.Z. and F.I.; Project administration, S.A.C. and F.I.; Resources, D.S. and Y.B.Z.; Software, F.I.; Supervision, S.A.C. and Y.B.Z.; Writing—original draft, P.B. and D.S.; Writing—review & editing, F.I. and Y.B.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research has been conducted by the Research Grant of Kwangwoon University, Seoul, Korea, in 2021.

Conflicts of Interest: The authors declare no conflict of interest in the publication of this paper.

References

1. 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]
2. Guha, A.; Samanta, D.; Banerjee, A.; Agarwal, D. A deep learning model for Information Loss Prevention from multi-page digital documents. *IEEE Access* **2021**, 9, 80451–80465. [CrossRef]
3. Hurley-Smith, D.; Wetherall, J.; Adekunle, A. SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 2927–2940. [CrossRef]

4. Afzal, M.K.; Rehmani, M.H.; Zikria, Y.B.; Ni, Q. Data-Driven Intelligence in Wireless Networks: Issues, Challenges, and Solution. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3722. [CrossRef]
5. 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]
6. 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]
7. 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]
8. Biswal, A.K.; Singh, D.; Pattanayak, B.K.; Samanta, D.; Yang, M.H. IoT-Based Smart Alert System for Drowsy Driver Detection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6627217. [CrossRef]
9. Bhardwaj, A.; El-Ocla, H. Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks. *IEEE Access* **2020**, *8*, 177534–177548. [CrossRef]
10. Paranthaman, V.V.; Kirsal, Y.; Mapp, G.; Shah, P.; Nguyen, H.X. Exploiting Resource Contention in Highly Mobile Environments and Its Application to Vehicular Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 3805–3819. [CrossRef]
11. 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]
12. Zhang, Y.; Shi, Y.; Shen, F.; Yan, F.; Shen, L. Price-Based Joint Offloading and Resource Allocation for Ad Hoc Mobile Cloud. *IEEE Access* **2019**, *7*, 62769–62784. [CrossRef]
13. Sivakumar, P.; Nagaraju, R.; Samanta, D.; Sivaram, M.; Hindia, M.N.; Amiri, I.S. A novel free space communication system using nonlinear InGaAsP microsystem resonators for enabling power-control toward smart cities. *Wirel. Netw.* **2020**, *26*, 2317–2328. [CrossRef]
14. Khamparia, A.; Singh, P.K.; Rani, P.; Samanta, D.; Khanna, A.; Bhushan, B. An internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e3963. [CrossRef]
15. Althar, R.R.; Samanta, D. The realist approach for evaluation of computational intelligence in software engineering. *Innov. Syst. Softw. Eng.* **2021**, *17*, 17–27. [CrossRef]
16. Jevtic, N.J.; Malnar, M.Z. Novel ETX-Based Metrics for Overhead Reduction in Dynamic Ad Hoc Networks. *IEEE Access* **2019**, *7*, 116490–116504. [CrossRef]
17. Liu, J.; Xu, Y.; Li, Z. Resource Allocation for Performance Enhancement in Mobile Ad Hoc Networks. *IEEE Access* **2019**, *7*, 73790–73803. [CrossRef]
18. Guha, A.; Samanta, D. Hybrid Approach to Document Anomaly Detection: An Application to Facilitate RPA in Title Insurance. *Int. J. Autom. Comput.* **2021**, *18*, 55–72. [CrossRef]
19. 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]
20. Anand, A.; Aggarwal, H.; Rani, R. Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks. *J. Commun. Netw.* **2016**, *18*, 938–947. [CrossRef]
21. Venkanna, U.; Agarwal, J.K.; Velusamy, R.L. A Cooperative Routing for MANET Based on Distributed Trust and Energy Management. *Wirel. Pers. Commun.* **2015**, *81*, 961–979. [CrossRef]
22. 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]
23. Biswas, J.; Kayal, P.; Samanta, D. Reducing Approximation Error with Rapid Convergence Rate for Non-Negative Matrix Factorization (NMF). *Math. Stat.* **2021**, *9*, 285–289. [CrossRef]
24. Samanta, D.; Alahmadi, A.H.; Karthikeyan, M.P.; Khan, M.Z.; Banerjee, A.; Dalapati, G.K.; Ramakrishna, S. Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture. *IEEE Access* **2021**, *9*, 98013–98025. [CrossRef]
25. 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]
26. 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]
27. Kumar, R.; Kumar, R.; Samanta, D.; Paul, M.; Kumar, V. A combining approach using DFT and FIR filter to enhance impulse response. In Proceedings of the 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 18–19 July 2017; pp. 134–137. [CrossRef]
28. Samanta, D.; Galety, M.G.; Shivamurthaiah, M.; Kariyappala, S. A Hybridization Approach based Semantic Approach to the Software Engineering. *TEST Eng. Manag.* **2020**, *83*, 5441–5447.
29. 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]

30. Mekala, M.S.; Patan, R.; Islam, S.H.; Samanta, D.; Mallah, G.A.; Chaudhry, S.A. DAWM: Cost-Aware Asset Claim Analysis Approach on Big Data Analytic Computation Model for Cloud Data Centre. *Secur. Commun. Netw.* **2021**, *2021*, 6688162. [CrossRef]
31. Dhanush, V.; Mahendra, A.R.; Kumudavalli, M.V.; Samanta, D. Application of deep learning technique for automatic data exchange with air-gapped systems and its security concerns. In Proceedings of the 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 18–19 July 2017; pp. 324–328. [CrossRef]
32. Gurunath, R.; Agarwal, M.; Nandi, A.; Samanta, D. An Overview: Security Issue in IoT Network. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018; pp. 104–107. [CrossRef]
33. 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]
34. Musaddiq, A.; Zikria, Y.B.; Ali, R.; Rasool, I.U.; Kim, S.W. Congestion control routing using optimal channel assignment mechanism in wireless mesh network. In Proceedings of the 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy, 4–7 July 2017; pp. 355–360. [CrossRef]
35. Zikria, Y.B.; Nosheen, S.; Kim, S.W. Quality of service analysis for multimedia traffic using DSR, AODV and TORA over Wi-Media ultra wide band. In Proceedings of the 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 13–17 January 2015; pp. 539–546. [CrossRef]