Lightweight Cryptography Model for Overhead and Delay Reduction in the Network

Rajesh Yamparala(✉) and T. Kamaleshwar

Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu 600062, India
rajeshyamparala@gmail.com

Abstract. Mobile Ad hoc Network (MANET) refers to a group of multi-hop wireless networks that can configure themselves. The success of MANET-based applications hinges on a number of criteria, with reliability being a key one. While many security procedures already exist, the new characteristics and vulnerabilities of this networking paradigm may make the old ones obsolete. The ability of a network to scale up in size without sacrificing performance is known as scalability. Proactive routing algorithms in mobile wireless networks face a significant scalability difficulty due to the frequent need to send and receive control signals. The key to fixing the scalability issue is cutting down on overhead. In order to lessen the burden of data transmission, a overhead and delay reduction model is designed in this research. The suggested technique is based on a weight function that integrates the node's connection and battery life. In this research, MANET network latency and traffic load reduction model is designed. The proposed technique is based on the idea of only transmitting certain, predetermined packets avoiding loss. Congestion in the network can be avoided by first ensuring that all neighbor nodes are valid before sending a packet. When it comes to the evolution of MANET, Quality of Service (QoS) is a crucial factor. This research proposes a Trusted Node Feedback based Node Authentication Model with Node Transmission Analysis (NAM-NTA) model for decreasing the network overhead and delay levels in the MANET. The emphasis of this research is on constraints based on latency and neighbor connectivity. This technique is able to detect superfluous connections and eliminate them from the network structure. The proposed achieved 98.3% accuracy in network delay reduction. The proposed model is compared with the traditional model and the results show that the proposed model performance in overhead and delay reduction is high.

Keywords: Mobile Ad hoc Network · Trusted Nodes · Node Authentication · Network Overhead · Network Delay · Node Feedback · Quality of Service

1 Introduction

A MANET, also known as a mobile communication network, is a network of mobile devices that connects to one another wirelessly and manages itself [1]. Multi-hop communication channels are used in a MANET [2]. Eventually, it will not be feasible or

P. Pareek et al. (Eds.): IC4S 2023, LNICST 536, pp. 362–375, 2024.
https://doi.org/10.1007/978-3-031-48888-7_31

even physically practicable to have a set architectural for this kind of network due to the rapidly evolving nature of wireless communication technology [3]. Due to the constantly shifting nature of the mobile structure, ad hoc wireless networks require the ability to self-organize and self-configure [4]. A MANET is a wireless network that establishes connectivity through multi-hop peer-to-peer routing rather than fixed network infrastructure [5]. MANETs find use in highly mobile and ever-changing military and civilian infrastructure. In a MANET, the structure of the network is dynamic [6].

MANETs are made up of a group of freely moving nodes. These nodes require no supporting infrastructure and can spontaneously form networks of any desired configuration [7]. Designing and implementing dynamic routing protocols with lower overhead and higher speed is a significant challenge in MANETs. For mobile ad hoc networks, researchers have developed a number of routing protocols, including Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) [8]. Any network can be transformed into a MANET by connecting a group of mobile wireless devices together. Every moving node can act as a host as well as a router [9]. The wireless interface has a limited broadcast range because data packets must travel from their source to their destination via a series of intermediate nodes. In a MANET, packets are sent from one node to another without the use of a central hub or other infrastructure [10]. As a result, MANET can be used where a wired network would be dangerous or impractical. In addition, it is used in challenging environments where it would be impractical to replace the batteries in any of the nodes. As a result, the packet forwarding process relies heavily on the routing protocol [11]. The structure of a MANET is shown in Fig. 1.

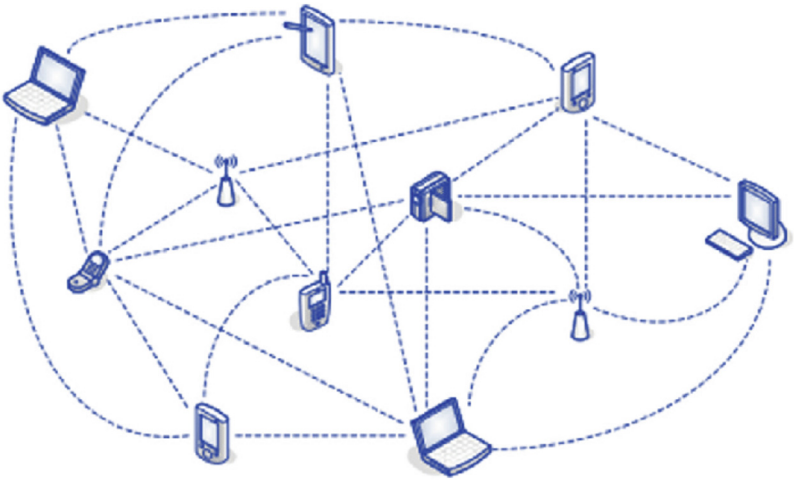

Fig. 1. MANET Structure

Ad hoc networks are becoming increasingly common in numerous contexts, including on military battlefields [12] to set up information networks between soldiers, weapon systems, command control centre, and vehicles due to their adaptability and ease of deployment [13]. Many real-time commercial applications are using the ad hoc network

architecture to boost productivity and effectiveness and optimize profits for their respective corporations. These applications are used in a wide variety of situations and services [15], including tactical networks, disaster relief, [14], home the environment, education system, recreation, sensor network, and context aware services. Link failure among nodes, lack of centralized administration in the absence of infrastructure, susceptibility to attack, high power consumption, low bandwidth, scalability of the network [16], device homogeneity, multi-hop routing, self-creation, autonomy, and self-administration are just some of the problems that need to be studied in order to be solved [17]. Many researchers have developed numerous solutions to the problem of network overhead and delay by utilizing transmission requirements for energy [18], residual consumption of electricity, or both.

The nodes in a MANET are mobile computers that can move around and connect with other nodes in the network over wireless links that can go in both directions [19]. The current approach in MANET relies on cooperation between nodes to allow for long-distance communication by forwarding each other's data packets [20]. However, even in cooperative settings, some nodes can refuse to do so in order to conserve power or to purposefully disrupt regular communications, which in turn reduces the efficiency of the network [21]. This kind of malicious activity is known as a packet dropping attack or black hole attack [22], and it is one of the most serious types of attacks that can bring down a network. In order to reduce the routing cost, these strategies are used to identify selfish nodes, bypass them, and select an alternative path for data transmission. Massive routing overhead is produced after switching to an alternative method for data transmission [23]. As a result, the innovative trans-mission method is implemented in this research to reduce routing overhead and improve network stability avoiding delay [24].

The processing delay in a packet-switched network is the time it takes for routers to process a packet's header. Delays in processing time are a major cause of overall network slowness. While handling a packet, routers can perform several functions, including determining the next hop for the packet and checking for bit-level errors that may have happened during transmission. High-speed routers often have processing delays on the microsecond scale or less [25]. The router then sends the packet to a queue, where it may experience additional waiting time after undergoing nodal processing. Delay in the transport of a packet is a concept fundamental to packet switching. The network-wide transfer or buffering delay of a packet is equal to the sum of the store-and-forward delays it encounters in each router. Network congestion and the quantity of intermediate routers both contribute to overall packet transfer latency.

2 Literature Survey

To extend the life of wireless multihop networks in which individual nodes experience an energy deficit, Choi et al. [1] applied wireless power transfer (WPT) technology to multihop transmission. The author has developed a system model for CoWPT-based multihop transmissions and posed an optimization problem to determine the optimal WPT time of each node in order to extend the network's lifetime. The net-work's longevity is guaranteed by first making sure all nodes have the same expected lifetime. To make

things easier, the author tackled the resulting linear programming (LP) problem instead of the optimization problem. Extensive simulations show that, compared to the normal WPT method, using the optimal CoWPT solution significant-ly extends the lifetime of networks in both WSN and MANET environments.

During mobile edge computing, connection failure is caused by node movement and decreased node energy, which in turn reduces the lifespan of the underlying mobile ad hoc network. Network latency grows dramatically when a route fails because route discovery must start afresh for single-path protocols. The proposed multi-path routing system is advantageous since it eliminates the need for route discovery. This study proposes LLECP-AOMDV, an ad hoc on-demand multi-path distance vector (AOMDV) routing protocol for mobile edge computing that is based on the prediction of connection lifetime and energy consumption. During the course of the path finding procedure, the energy grading method is utilized. When a node's energy gets too low, it stops participating in the route finding process. The routing selection process prioritizes paths with the lowest energy consumption and the longest predicted link lifetimes. The results of the comparisons were assessed by the author in terms of energy consumption, packet delivery rate, and end-to-end delay.

A mobile ad hoc network (MANET) is a loosely organized network of mobile, networked computers. Moving nodes increase route overhead and battery consumption, making mobile communication routing challenging. The field of MANET has made multiple attempts to reduce the energy consumption of nodes and the complexity of routing decisions. These concepts can improve load distribution and traffic flow while decreasing resource waste. The unique idea provided by Chandravanshi et al. [3] has the potential to yield better outcomes. Author proposes an adaptive Multipath Multichannel Energy Efficient (MMEE) routing approach in which route selection strategies are based on the expected energy usage per packet, bandwidth available, queue length, and channel utilization. Multipath reduces the probability of collisions by assigning data packets to different paths throughout a network, whereas multichannel employs a channel ideal assignment technique to reduce collisions between nodes. The multichannel approach divides the bandwidth of a link into multiple discrete channels. To reduce network collision, multiple source nodes can consume the channel bandwidth simultaneously. Through the use of a collaborative multipath multi-channel method, data can go from several sources to the same destination without experiencing collisions or congestion. The MMEE routing strategy is used to deter-mine which routes to take. The proposed MMEE improves network dependability by selecting the path using a load and bandwidth aware routing algorithm that takes into account the energy and predicted lifetime of individual nodes.

Of-floading computing from the edge is a challenging problem in 5G and 6G research since edge cloud services are not always available in outlying areas. Instead of investing in costly infrastructure to provide edge computing services in these areas, drones might be used instead. Due to limitations in drone range, it is challenging to provide effective edge computing services. Feng et al. [4] developed an edge computing architecture where drones with and without edge servers work cooperatively to provide edge computing services to end users, with computing activities conveyed in a Mobile Ad hoc Network through multi-path and multi-hop. Extending the lifetime of

a MANET while maintaining service quality is defined as a joint optimization issue involving the selection of computational drones, transmission paths, and task division schemes. Because of its ability to achieve an incomplete remedy to the problem via a greedy strategy, a Software-Defined-Network (SDN) controller is employed to investigate the issue. Taking into account the dynamic nature of the MANET, the original issue is reframed as a multi-path multi-hop task transmission problem with an arrival order constraint on the tasks to be executed.

Vehicle ad hoc networks (VANETs), UAV ad hoc networks, and wireless sensor networks are just a few examples of MANETs that benefit from the decentralized and mobile nature of the transparent architecture. There is a wealth of information available on the topic of building decentralized scheduling algorithms for topology-agnostic MANETs. Most of them do their analyses in completely delay-free settings. The requirement for MANETs to support time-sensitive traffic is only going to in-crease as more and more real-time applications switch to wireless communications. If a packet hasn't been sent within a certain amount of time, it is erased from the sys-tem regardless of its status. Compared to the regular delay-free version, this is light years ahead. To address the issue of accommodating time-sensitive traffic, Deng et al. [5] investigated distributed scheduling strategies for a topology-agnostic MANET. We compare the probabilistic ALOHA scheme to the more traditional TDMA, Chlamtac and Farag's GF sequence scheme, and a combination sequence scheme designed for a certain type of sparse network topology.

Despite named data networking's (NDN) promising benefits for MA-NETs, its deployment is hindered by MANETs' distinctive features and architectural incompatibilities. Due to the fixed nature of data routers and the prevalence of servers in NDN's role as providers, FIBs there tend to be stable. FIBs are often unreliable in MANETs because of the unpredictable behavior of mobile nodes acting as both data routers and providers. Too frequent updates to the FIB might cause data acquisition failures by causing a broadcast storm and out-of-date FIBs. In addition, NDN's reverse path-ways are extremely reliable because static data routers are used to build them. Disruptions on reverse paths are common in MANETs since they are made up of mobile nodes. The costs and time involved in data recovery are high, and data gathering failures are common as a result. With the intention of improving data collection success rates and reducing data acquisition expenses, Wang et al. [6] proposed an efficient data acquisition method for NDN-based MANET. The concept has mobile nodes retrieve information without using FIBs and then distribute it to multiple users. Data continuity and successful reception on the outbound path are also guaranteed, along with mobility support.

When a natural disaster occurs, the normal communication infrastructures are immediately destroyed. Intermittently connected MANETs are essential for providing network access in the aftermath of a disaster. Despite the fact that the majority of previous study on such networks has focused on one-to-one chat, the significance of monitoring apps has expanded in recent years. In monitoring applications, the timeliness of the data is more significant than its delay characteristics. A mathematical assessment of the age of information (AoI) was proposed by Inoue et al. [7] for MA-NETs with intermittent connectivity; this study would capture the timely nature of data collected by monitoring programs. The author used the results of the analysis to go into the basics of network architecture.

Transmission reuse, or the cooperation of the various destinations, is the primary advantage of multicast over multi unicast. Multicast's ability to increase transmission efficiency stems from this feature. This has led to extensive study of multicast in a variety of wireless contexts. When using multicast rather than multiple unicast, the implications of node mobility on transmission reuse are better known. Correlated mobility, a phenomena that faithfully replicates real-world mobility processes, is the focus of Jia et al. [8], who want to clarify the effect of mobility on transmitter reuse in mobile ad hoc networks. The multicast gain was employed by the author as a metric of transmission reuse since it represents the capacity ratio of multimedia to multi unicast under a particular delay limitation. By developing a multi-layer routing proto-col and presenting many causal scheduling techniques, we can examine the impact of different correlation degrees of node mobility on the total multicast capacity delay tradeoff. The capacity and delay advantages of multicasting are calculated and compared to the unicast scenario.

3 Proposed Model

Nodes in MANETs can function as both a source and a sink, making this type of network highly adaptable. Memory, power, and network buffers are just a few examples of scarce resources for mobile nodes. Information interchange, path selection, and routing are only few of the procedures that use up these resources. When the nodes take on the role of routers, they must communicate with one another to share and improve their routing knowledge. The network's performance, durability, and convergence can all be kept at satisfactory levels with the help of control data. Nodes rely heavily on control data to maintain an accurate routing table. Depending on the routing protocol in use, the control data may exchange multiple short packets to ascertain the accessibility of surrounding nodes, for instance.

Nodes in a MANET are characterized by their minimum requirements for transmission power, distribution, mobility, and memory. Due to the limited transmission range, path of minimum hop, minimum normalized residual energy used, minimal level absolute remaining energy used, minimum transmission energy path, throughput, bandwidth, hop count, and power to be sufficient, the wireless mobile nodes enter and leave the network dynamically in MANETs. In a typical network, information travels via several intermediate nodes before reaching its intended destination. Since each mobile ad hoc network node must contribute to network traffic that is unrelated to its own needs, a router is required to keep packets flowing smoothly. Congestion control is essential in MANETs to prevent packet loss, boost network energy, and lower overhead costs, all of which can be attributed to the high volume of traffic. Congestion happens when there are more packets trying to travel across a network than the network can handle at once. Without a fixed network, mobile nodes can talk to one another using radio links. The proposed model framework is shown in Fig. 2.

Control routing refers to the transmission of routing and control data into a network, and it is essential for network resilience. To achieve rapid convergence, it is necessary to inform all nodes in the network if there is a change in the network path due to link failure or busy nodes. Overhead refers to the portion of a transmission that consists of control routing rather than data. To maintain an appropriate degree of overhead without

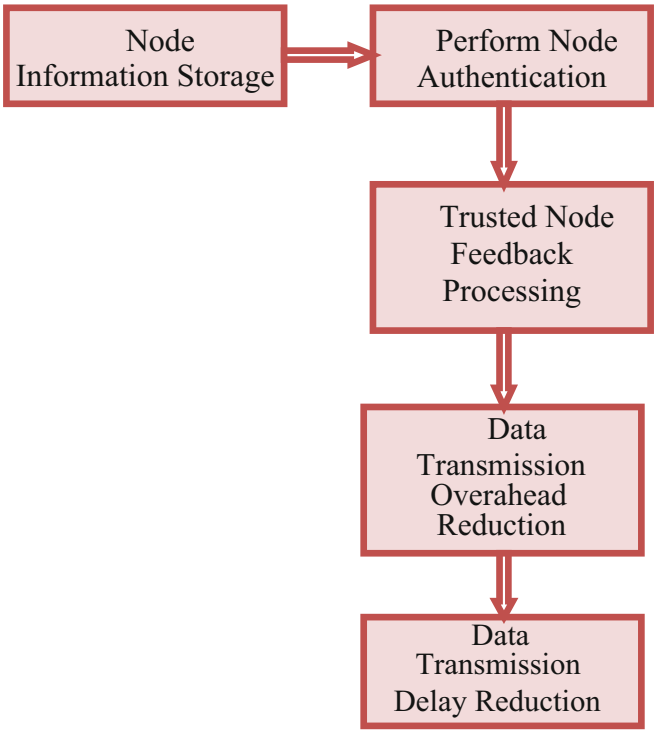

Fig. 2. Proposed Model Framework

sacrificing throughput is a key network objective. If the network's overhead is low, it will employ its maximum effective throughput at the expense of reliability. While adding more overhead improves reliability, it slows effective throughput. Because of the nodes' mobility, more control routing operations need to be performed in ad hoc networks, leading to a high level of overhead. When nodes are moved, the network's topology is constantly being reconstructed since the end-to-end path is altered. This proposal evaluates the effects of various ad hoc routing protocols by measuring certain indicators across the network. There are two main categories for metrics: reliability and overhead. Measures of reliability include throughput, packet loss, delay and round-trip time. Overhead behavior and cumulative overhead are features of the overhead set method. This research proposes a Trusted Node Feedback based Node Authentication Model with Node Transmission Analysis (NAM-NTA) model for decreasing the network overhead and delay levels in the MANET.

Initially the nodes that need to participate in ad hoc communication information is maintained in the selected node in the network that has high performance in the past data transmissions. The node information is maintained as

$$Nodeinfo[NodeList] = \sum_{n=1}^{NodeList=K} \frac{getnodeaddress(n)}{maxlimit(NodeList)} + allocenergy(n) + \tau(n) \tag{1}$$

$$NodeKey[K] = \prod_{n=1}^{K} \frac{maxener(n)}{\lambda} + getTime(n) + Nodeinfo(n) \tag{2}$$

τ is the node computational level to allocate tasks to the node. The node address is gathered for future communication. λ is the total energy allocated.

The node authentication is performed by using light weight cryptography models that is used to validate the nodes during data transmission and receiving. The process of node authentication is performed as

$$\begin{aligned} NodeAuthen[K] &= \sum_{n=1}^{K} Nodeinfo(n) + getnodeaddress(n) \\ &+ \begin{cases} if\ NodeKey(n) == getNodeKey(n)\ return\ access \\ Otherwise \qquad\qquad\qquad\qquad remove(n) \end{cases} \end{aligned} \tag{3}$$

The trust factor of nodes helps in detection of malicious actions in the network. For each node, its adjacent node feedback about the current node is considered as an important parameter in node usage in data transmission. The trusted node feedback is calculated in quick packet delivery rate to avoid delay. The process is performed as

$$\begin{aligned} TfNeigh[K] &= \prod_{n=1}^{K} getmaxPDR(n+1) + enercons(n+1) \\ &+ \max(\tau(n+1)) \begin{cases} Tf = 1\ if\ (TFNeigh(n) > Th) \\ 0 \qquad\qquad\qquad\qquad Otherwise \end{cases} \end{aligned} \tag{4}$$

Overhead in MANET is any unneeded consumption of time, space and energy in data transmission. Overhead is the additional storage needed for supporting data that facilitates the conveyance of a particular message from a source to a receiver. The overhead during data transmission is calculated as

$$\begin{aligned} Ovrhd[K] &= \sum_{n=1}^{K} getTime(\gamma) - getTime(\gamma+1) + \omega(n, n+1) \\ &+ Th \begin{cases} if\ Ovrhd(n) > Th\ return\ 1 \\ otherwise \qquad\qquad return\ 0 \end{cases} \end{aligned} \tag{5}$$

γ is the data transmission levels of the current node to the next node. ω is the delay levels of the transmission among current and next trusted neighbor nodes.

There are several potential sources of network delays in any given communication system. The distance here between origin and the target is the most fundamental factor. Nevertheless, the information does not move straight from one location to another. Several intermediate nodes along its route will add to the transmission time. The delay level caused by malicious nodes in the network is calculated as

$$DelayL[K] = \prod_{n=1}^{K} \frac{\tau(n, n+1) + minLoss(n)}{\max(PDR)} + \max(Ovrhd(n, n+1)) - Th \tag{6}$$

4 Results

Nodes in a mobile ad hoc network communicate wirelessly and independently. Using MANET, a temporary network can be formed without the need for a single point of control. This is because nodes in a MANET tend to move around a lot. There are many instances of broken connections and blocked pathways. If a mobile node can't determine the path to its target, it will blindly retransmit the route request packets to its adjacent nodes, resulting in a broadcast storm. A rebroadcast delay model to decide rebroadcast order, define a connectivity factor to maintain network connectivity, and establish a rebroadcast probability to maximize the use of neighbor coverage knowledge is proposed. Because of this, the overhead is decreased and the network performance is improved because to the synergy between neighbor coverage knowledge and the probabilistic approach.

This research ultimate goal is to design a energy-efficient data transmission protocol for MANET, which significantly increases the network's lifetime. Using the available protocol methods with increased transmission coverage range of relay nodes, MANET devices are able to keep the network running on a restricted battery supply. However, when compared to direct transmission protocol idea methods, cooperative communication protocol methods have not always been successful energy efficient approaches to increasing the transmission range of intermediate relay nodes with less power consumption. This research proposes a Trusted Node Feedback based Node Authentication Model with Node Transmission Analysis (NAM-NTA) model for decreasing the network overhead and delay levels in the MANET. The proposed model is compared with the traditional Lifetime Maximization in Wireless Multihop Networks (LMWMN) model and the results represent that the proposed model performance is high in delay and overhead reduction.

The nodes in the network that need to participate in data transmission will provide the node information to the monitoring authority in the network. This information helps in recognition of nodes in transmissions. The Network Node Information Storage Time Levels in milliseconds of the existing and proposed models are shown in Fig. 3.

Each node in the network will be authenticated with the unique key provided after information storage in the network. The unique key helps in recognition of malicious nodes in the network. The node authentication helps in maintaining access control only for the authorized users. The Node Authentication Accuracy Levels in percentage of the proposed and existing models are shown in Fig. 4.

The trust factors calculated in the nodes helps in consideration of only trusted nodes and neighbor feedback is considered only from the trusted nodes. The feedback helps in detection of malicious actions in the network and such activities can be avoided to increase the network lifetime. The Trusted Node Feedback Gathering Time Levels of the proposed and existing models are depicted in Fig. 5.

The sum total of all throughput, energy, storage, time, etc. consumed by all sensor nodes in the network is called overhead. The network overhead plays a major role in performance of the network. The minimum the overhead, the maximum the performance is. The proposed model as it considers the neighbor feedback and detects the malicious actions, the data transmission is also performed in active state and then nodes enters into inactive state in which the usage of the resources is reduced and balanced. The

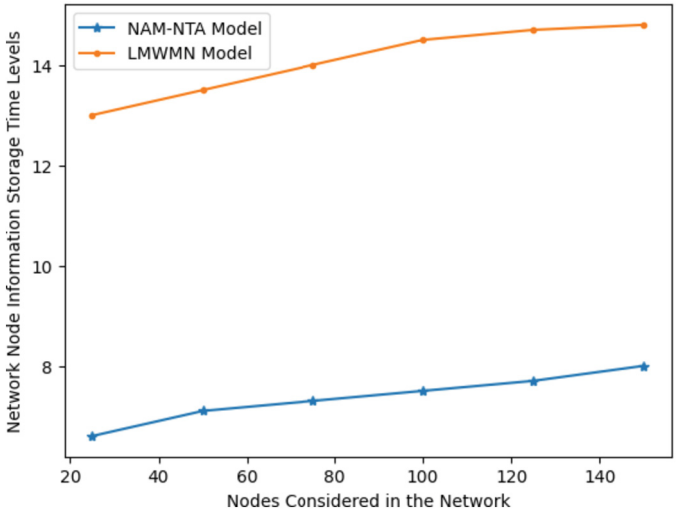

Fig. 3. Network Node Information Storage Time Levels in Milliseconds

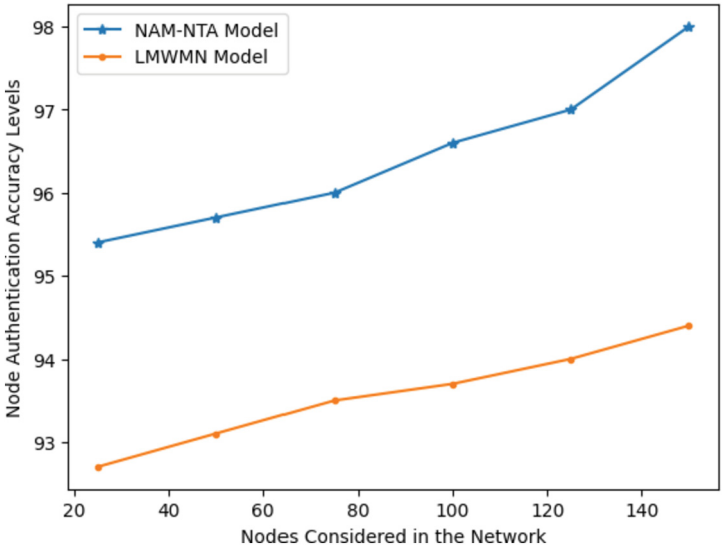

Fig. 4. Node Authentication Accuracy Levels in Percentage

Fig. 6 shows the Network Overhead Reduction Time Levels of the existing and proposed models.

A MANET network delay is a function of its design and operation. It defines the time it takes for data to go from one trusted node to another in a network. Multiplied or fractional seconds are common units of measurement. Network latency is the overall time required for a message to travel from sender to receiver, whereas propagation delay

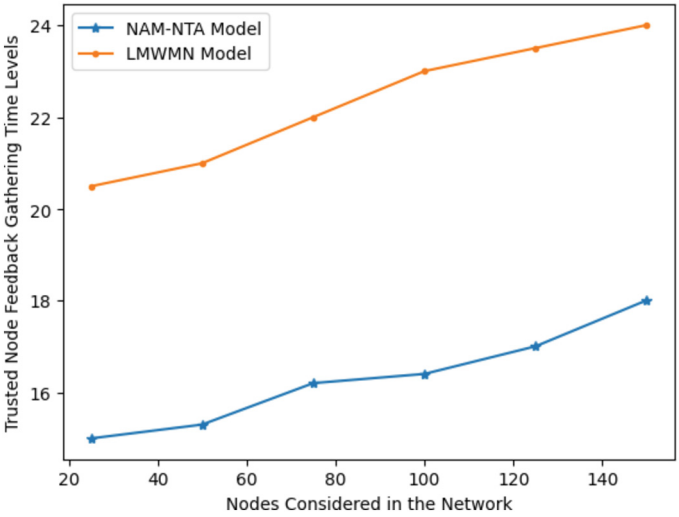

Fig. 5. Trusted Node Feedback Gathering Time Levels

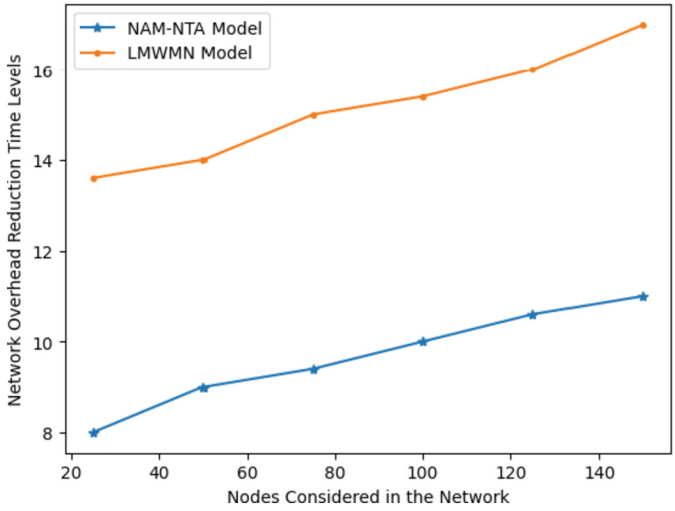

Fig. 6. Network Overhead Reduction Time Levels

is the process required the initial bit to transit over a link. The Network Delay Level Reduction Accuracy Levels of the existing and proposed models are shown in Table 1 and Fig. 7.

Table 1. Accuracy Levels

Nodes considered in the Network	Models Considered	
	NAM-NTA Model	LMWMN Model
20	96.2	90.2
40	96.3	91
60	97.3	91.3
80	97.6	91.7
100	98	92
120	98.1	92.1
140	98.3	92.4

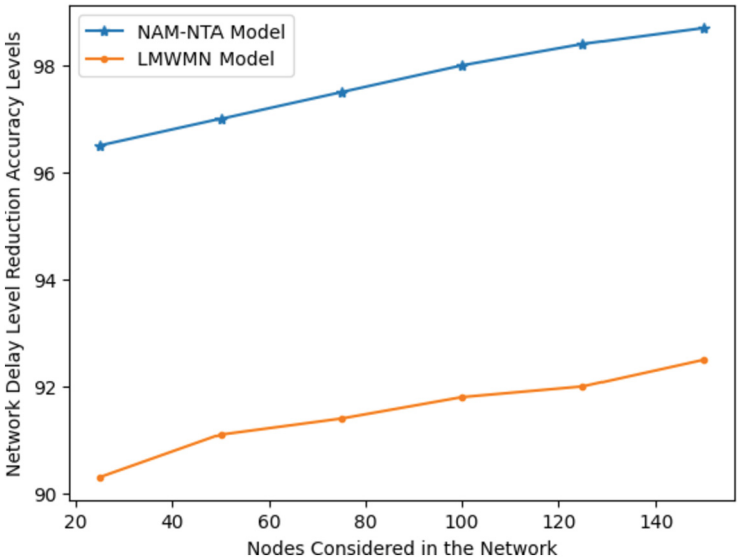

Fig. 7. Network Delay Level Reduction Accuracy Levels

5 Conclusion

The nodes in MANETs can move around freely. The nodes have complete mobility. Without a predetermined framework, these nodes are capable of dynamically self-organizing into networks of any desired topology. MANETs suffer from frequent link breakages since their nodes are constantly moving around. This resulted in several route discoveries and path failures. The time and effort required to find a new path must be taken into account. Broadcasting is an essential and efficient tool for disseminating information during the route finding process. Important network environments that greatly affect the performance of routing protocols in MANETs include power, mobility, topology, and

node density. Due to their wireless nature and the fact that the nodes interact with one another via multi-hop routing, mobile ad-hoc networks are highly adaptable and independent of any central infrastructure. The majority of currently-used MANET routing methods are designed for networks in which every node has the same data transfer and processing capabilities. In terms of MANET scalability, homogeneous networks perform poorly compared to heterogeneous networks despite being simpler to model and investigate. This research proposes a Trusted Node Feedback based Node Authentication Model with Node Transmission Analysis model for decreasing the network overhead and delay levels in the MANET. The proposed model achieves 97% accuracy in overhead and delay reduction. The proposed in future can be enhanced by designing a malicious node detection models for removing such nodes for performance enhancement. The proposed model also can be extended for clusters generation and data transmission with secured node authorization models.

References

1. Choi, H.-H., Lee, K.: Cooperative wireless power transfer for lifetime maximization in wireless multihop networks. IEEE Trans. Vehic. Technol. **70**(4), 3984–3989 (2021)
2. Zhang, D.-G., et al.: A multi-path routing protocol based on link lifetime and energy consumption prediction for mobile edge computing. IEEE Access **8**, 69058–69071 (2020)
3. Chandravanshi, K., Soni, G., Mishra, D.K.: Design and analysis of an energy-efficient load balancing and bandwidth aware adaptive multipath N-channel routing approach in MANET. IEEE Access **10**, 110003–110025 (2022)
4. Feng, G., Li, X., Gao, Z., Wang, C., Lv, H., Zhao, Q.: Multi-path and multi-hop task offloading in mobile Ad Hoc networks. IEEE Trans. Vehic. Technol. **70**(6), 5347–5361 (2021)
5. Deng, L., Liu, F., Zhang, Y., Wong, W.S.: Delay-constrained topology-transparent distributed scheduling for MANETs. IEEE Trans. Vehic. Technol. **70**(1), 1083–1088 (2021)
6. Wang, X., Lu, Y.: Efficient forwarding and data acquisition in NDN-Based MANET. IEEE Trans. Mob. Comput. **21**(2), 530–539 (2022)
7. Inoue, Y., Kimura, T.: Age-effective information updating over intermittently connected MANETs. IEEE J. Select. Areas Commun. **39**(5), 1293–1308 (2021)
8. Jia, R., Lin, F., Zheng, Z.: Exploring the impact of node correlation on transmission reuse in MANETs. IEEE Access **8**, 12607–12621 (2020)
9. Veeraiah, N., et al.: Trust aware secure energy efficient hybrid protocol for MANET. IEEE Access **9**, 120996–121005 (2021)
10. Durr-e-Nayab, Zafar, M.H. and Altalbe, A.: Prediction of scenarios for routing in MANETs based on expanding ring search and random early detection parameters using machine learning techniques. IEEE Access **9**, 47033–47047 (2021)
11. Fan, R., Atapattu, S., Chen, W., Zhang, Y., Evans, J.: Throughput maximization for multi-hop decode-and-forward relay network with wireless energy harvesting. IEEE Access**6**, 582–24 (2018)
12. Noor, M.B.M., Hassan, W.H.: Current research on Internet of Things (IoT) security: a survey. Comput. Netw. **2019**(148), 283–294 (2019)
13. Arvind, S., Narayanan, V.A.: An overview of security in CoAP: attack and analysis. In: Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 655–660, Coimbatore, India (2019)
14. Surendran, S., Nassef, A., Beheshti B D.: A survey of cryptographic algorithms for IoT devices. In: Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1–8, Farmingdale, NY, USA (2018)

15. Kumar, P., Yun, L., Guangdong, B., Andrew, P., Jin, S.D., Andrew M.: Smart grid metering networks: a survey on security, privacy and open research issues. IEEE Commun. Surv. Tutor. **21**, 2886–2927 (2019)
16. Abosata, N., Al-Rubaye, S., Inalhan, G., Emmanouilidis, C.: Internet of Things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors **21**, 3654 (2021)
17. Sarenche, R., Salmasizadeh, M., Ameri, M.H., Aref, M.R.: A secure and privacy-preserving protocol for holding double auctions in smart grid. Inf. Sci. **2021**(557), 108–129 (2021)
18. Abdallah, A., Xuemin, Sherman S.: A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans. Smart Grid **9**, 396–405 (2018)
19. Khan, A., Vinod, K., Musheer, A., Saurabh, R.: LAKAF: lightweight authentication and key agreement framework for smart grid network. J. Syst. Archit. **116**, 102053 (2021)
20. Abbasinezhad-Mood, D., Nikooghadam, M.: An anonymous ECC-based self-certified key distribution scheme for the smart grid. IEEE Trans. Ind. Electron. **2018**(65), 7996–8004 (2018)
21. Grover, H.S., Kumar, D.: Cryptanalysis and improvement of a three-factor user authentication scheme for smart grid environment. J. Reliab. Intell. Environ. **2020**(6), 249–260 (2020)
22. Braeken, A., Kumar, P., Martin, A.: Efficient and provably secure key agreement for modern smart sensoring communications. Energies **11**, 2662 (2018)
23. Khan, A A., Kumar, V., Ahmad, M., Rana, S., Mishra, D.: PALK: password-based anonymous lightweight key agreement framework for smart grid. Int. J. Electr. Power Energy Syst. **121**, 106121 (2020)
24. Chaudhry, S.A.: Correcting PALK: password-based anonymous lightweight key agreement framework for smart grid. Int. J. Electr. Power Energy Syst. **125**, 106529 (2021)
25. Deng, L., Gao, R.: Certificateless two-party authenticated key agreement scheme for smart grid. Inf. Sci. **2021**(543), 143–156 (2021)
26. Chaudhry, S.A., Alhakami, H., Baz, A., Al-Turjman, F.: Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure. IEEE Access **8**, 101235–101243 (2020)
27. Jan, M.A., Khan, F., Alam, M., Usman, M.: A payload-based mutual authentication scheme for Internet of Things. Future Gener. Comput. Syst. **92**, 1028–1039 (2019)
28. Park, C.-S., Park, W.-S.: A group-oriented DTLS handshake for secure IoT applications. IEEE Trans. Autom. Sci. Eng. **15**, 1920–1929 (2018)
29. Abdullah, D., et al.: Super-encryption cryptography with IDEA and WAKE algorithm. J. Phys. Conf. Ser. **1019**, 012039 (2018)