SRTE: Security Resource Allocation for Trust Model in Evaluate the Strong Node

M. Anugraha
Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, India.
E-mail: grahaanu90@gmail.com

Dr.S.H. Krishnaveni
Associate Professor, Department of Computer Science and Engineering, Baselios Mathews II College of Engineering, Sasthamcotta, Kollam, India.
E-mail: shkrishnaveni@gmail.com

Received August 27, 2021; Accepted December 05, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19092

Abstract

Mobile ad hoc network (MANET) is a framework-free as well as self-designing network in which Mobile Nodes (MN) travel freely across the contact spectrum using cellular network interfaces. Through the advancement of wireless technologies, a complex network can better handle data communication protection while improving quality of service (QoS) metrics. MANET is defenceless to security breaches due to the absence of a trusted unified authority. In MANET, the SRTE approach, also known as protection allocation of resources for trust model, is introduced for evaluating strong nodes. Main contribution of the work have four parts: First, to improve secure data transmission in MANET’s environment, the H-ACO-DSR method is introduced. Second part, the HTDMA method is developed for better resource allocation. Third part, the HTCMR is introduced and produce the efficient cluster and trust worthiness in the MANET’s environment. Fourth part, the ABT is used to identify the malicious node and trusted Node in the system. To boost the Qos metric efficiency, the trusted nodes in MANET as well as data transmission are carried out with the trusted MN. Finally, as compared to current approaches, simulation results produce improved PDR and low cost Energy, Average Delay, Routing overhead, and Throughput.

Keywords

SRTE, MANET, QoS, Throughput and PDR.
Introduction

MANETs (Mobile Ad Hoc Networks) was among the most prominent research subjects in recent years. MANET is a completely distributed network that can operate in a variety of locations, but network association and message distribution must be handled by the nodes themselves. There are no fixed transportation requirements, such as entry points or base stations. The mobile ad hoc network is a form of decentralised network. The nodes in a mobile ad hoc network literally connect to form a network. Single-hop and multi-hop connectivity is feasible in the network, resulting in direct and indirect communication. Because two nodes are in proximity of each other, they can communicate directly (Bhattacharyya, 2011).

The three main problems in MANET routing, defence, and QoS that can be addressed in this studies to make communication more effective and secure came into existence recently. In a Mobile Ad hoc Network system, secure data sharing is a challenge one. Protection has not been taken into consideration or in certain aspects in standard MANET routing methods; security alerts have been handled without improving routing efficiency (Ergenc, 2019). In this article, the Hybrid Trust Model (HTM) in MANETs is proposed, and an optimization strategy called Ant Colony Optimization is used (ACO). In an ad hoc network, the ACO algorithm is an optimization strategy for designing routing algorithms. The shortest path from a source node to a neighbour node is found using the ACO algorithm. Finding the shortest path has become a major issue in today's mobile ad hoc network. To address this problem, the Ant Colony Optimization (ACO) technique is employed. Normally, this algorithm is based on Ant's action (Chatterjee, 2015). Whenever an ant travels from its nest to its meal, it emits a chemical called pheromone. By smelling the pheromone, the mentioned ants will discover the path. This pheromone would leave a trace on the ground surface, allowing the ant to track previous ants and find good food. The ACO algorithm is used in this paper to find the shortest path from a source node to a neighbour node while also including a key for each node. The nodes are kept safe by supplying a key to each one. Data replication, data degradation, and other problems can all be eliminated with key generation.

1. Organization of the Research Work

The remainder of the work is in the following order. The second section examines the associated films. The proposed methodology-based confidence assessment for safe communication in MANET is briefly described in Section 3. The simulation settings are
listed in Section 4. The simulation findings and comparative analysis are discussed in Sect. 5 using a number of metrics. The conclusion is found in Section 6.

**Research Review in Various Techniques**

The study of the research review have four steps they are, Security, Resource allocation, Trust model and evaluate the strong node. These studies are following below.

Ali, S. S., et al. (Ali, S. S.,2017) were added to improve the mobility and confidence level of the nodes. The three limits of a node's trust factor are the node's mobility, capacity, and past. In the mobility setting, the main restriction for having the right routing should be less than turnaround time. Routing in an ad-hoc network is often achieved as a three-way handshake, with the first broadcasting of a route request followed by route replay and then setting up the route. Rattrout et al. (Bhattacharyya, 2011) contributed to the system's increased stability. Some methods can alter MANET rules such as node speed, energy, and coverage. A measurement is required to change the system's topology and improve its security. Artificial Bee Colony is regarded as one of the network's most notable improved improvements. It will provide a model based on ABC that will aid in the selection of the system's head cluster category, which will be influenced by different parameters such as speed and energy. Since these boundaries are known as the key determinants of MANET topology. In the future, we will consider putting this model into action and comparing the results to those of other models.

Chatterjee et.al (Fan, Ziqi, 2011) have discussed and implemented E-Ant–DSR, idea of the routing techniques of development and self-association in natural frameworks. At that point the centers of productive routing maintains of the strategic distance from congestion and connection breakage wonders. Alongside the proficient routing, it likewise performs huge energy utilization. They compared the method to other ACO approaches and found that it provided superior results in terms of information distribution ratio, split path, routing overhead, as well as energy use. P-TDMA, a Markov Chain-based TDMA protocol for mesh networks, is proposed by Fan et al. (5. We show that P-TDMA performs admirably in both stable and strong situations as well as in weak and insecure situations. The schedule opening task for P-complex TDMA is problematic because it is based on the state of each time allotment for each end-client system. P-TDMA, in comparison to previous studies on the even schedule assignment strategy, will do well in a number of scenarios. By reducing the frame length of each node, the TDMA mechanism, as defined by Kanzaki et al. (Patel,2018), prevents the increase of unassigned slots. It also employs a frame length of a power of two to ensure collision-free packet communication.
between mobile hosts of varying frame lengths. We've also put our protocol into simulation testing to see how well it performs. According to the results, our protocol enhances channel use. Devi et al. (Bouyer, 2018) suggested the trust improved cluster based multipath routing (TECM-OLSR) convention to solve security concerns in MANETs. According to execution evaluation with the quantity of nodes shifting as well as node speed varying, the TECM-OLSR convention with changing number of adjustable nodes in the set region is more competitive than the FPNT-OLSR convention. As a consequence of the trust's security reliability, the routing of numerous malicious threats such as Sybil, Byzantine, Sinkhole, Wormhole, Black hole, Denial of service, and Jelly fish attacks is increased. Bouyer et al. (Ergenç, 2019) describe clustering methods that combine the KHM with a modified PSO measuring adaptation (MPSO) and an enhanced Cuckoo Search system (ECS) (MPSO). The bulk of other transforming calculations, such as PSO and SA, have a lower intermingling rate than normal CSA.

The research work contributes to overcoming the issues of the above-mentioned traditional approaches by designing for four steps: H-ACO-DSR improves security, HTDMA improves resource allocation in MANETs, HTCMR focuses on trustworthiness, and finally ABT evaluates strong nodes in the mobility setting.

- **Security (S):** To improve secure data transmission in MANET’s environment, the H-ACO-DSR method is introduced and produce the healthy data transmission.

- **Resource Allocation (RA):** To improve the system efficiency for node transmission to one cluster to another cluster, the HTDMA method is developed for better resource allocation.

- **Trust Model (TM):** To improve the data security and trusted node transmission in the cluster, the HTCMR is introduced and produce the efficient cluster and trust worthiness in the MANET’s environment.

- **Evaluate the Strong Node (ESN):** Evaluate the combine weak node into strong nodes in mobility environments, the ABT (**Adaptive Booting Technique**) is used to identify the malicious node and trusted Node in the system. Finally produce the healthy and efficiency of the system.
Methodology

The routing information is kept safe by MANET. However, preserving trust between nodes is a difficult problem in this work, so stability, Resource Allocation, Trust Model, and Strong Node are used to detect and assess these issues. The researchers have suggested many methods for attackers to locate these malicious nodes. In the context of mobile ad hoc networks (MANETs), secure data sharing is a challenging challenge. The power supply for these mobile nodes is provided by batteries, which must have a low energy consumption. The aim of data security is to prevent attacks on these nodes and data communication. Figure 1 depicts our proposed scheme, which is divided into four segments. The suggested solution encrypts the data before sending it to its final destination. It also helps to extend the longevity of mobile networks. Any of the parameters that we consider in our simulation work include connectivity, energy, average delay, throughput, and overall cluster efficiency. The simulation outcome illustrates a performance study of HTM's stable security, as well as how to maximise system reliability, quantify strong nodes, assess trustworthiness, and improve data transmission security.

Fig. 1 System Model

Security
Hybrid Ant Colony Optimization with DSR protocol (H-ACO-DSR)

Resource Allocation
Hybrid Time Division Multiple Access (H-TDMA)

Trust Model
Hybrid Trust Cluster based Multiple Routing (H-TCMR)

Evaluate Strong Node
Adaptive Booting Technique (ABT)
1. H-ACO-DSR (Hybrid Ant Colony Optimization with DSR Protocol)

In the present situation, coordination in handheld Ad hoc networks takes place in a variety of ways. A fixed infrastructure, such as a base station or an entry point, may be present in the network. Data will be sent from the nodes in this way to the base station, that will transmit it to the destination. Many issues would arise as a result of this, including packet loss, latency, capacity, overhead, throughput, packet distribution ratio, connectivity, malicious attackers, and so on. As a result, the Hybrid Trust Model detects and evaluates these problems. The nodes will send data one by one to the receiver through neighbour nodes in the shortest path using the Ant Colony Optimization (ACO) process. But, if there is any misbehaviour during this transmitting cycle, there is a chance that a packet will be dropped, and it will also take a long time to transmit the data, so the Dynamic Source Routing (DSR) protocol was created to solve this. DSR manages a server and a firewall. One node acts as a channel for two or three nodes, and the nodes send data to the channel, which is then checked to see if it is authenticated. Another node would function as a gateway, allowing authenticated data to be sent to the gateway and then to the destination using the shortest path possible. Data is encrypted and decrypted using the token. Symmetric key algorithms like DES and AES, as well as public key algorithms like RSA, are used in cryptographic schemes. For safe data transfer, this work uses AES (Advanced Encryption Standard) as a key (5). The AES encryption algorithm specifies a collection of transformations to be applied to data in an array.

Solution elements $c_{ij}$ the edges of the diagram, as well as the $\tau_{ij}$, the pheromone update, ie, the pheromone related with the combined edge of i as well as j cities is as follows:

$$\tau_{ij} \leftarrow (1 - \rho) \cdot \tau_{ij} + \sum_{k=1}^{m} \Delta \tau_{ij}^{k}$$ \hspace{1cm} (1)

$\rho \in (0,1)$ evaporation rate, where m is the number of ants, then $\Delta \tau_{ij}^{k}$ is the amount of pheromone given on the edge (i, j) by k-th ant:

$$\Delta \tau_{ij}^{k} = \begin{cases} \frac{1}{L^k} & \text{if, ant } k \text{ used, edge } (i,j) \text{in its tour,} \\ 0 & \text{otherwise}, \end{cases}$$ \hspace{1cm} (2)

The length of the k-ants is given by $L^k$. In managing solutions, ants cover the construction map and take a stimulating decision at each end.
Algorithm

Step 1: Set basic parameters such as ants, independent tests, and number of tours in each trial.
Step 2: Place all the ants in randomly different user.
Step 3: \( \tau_{ij} = 0 \) Pheromone tracking is zero in the initial step.
Step 4: Initially the tabu list = \{i\} (the present user).
Step 5: Each ant moves through the next user probability function.
\[
p_{ij}^k(t) = \begin{cases} 
\tau_{ij}(t)^\alpha (\eta_{ij})^\beta & \text{if } j \text{allowed}_k \\
0 & \text{else}
\end{cases} 
\]
Where,
\( p_{ij}^k(t) \) = Probability of moving from user ‘i’ to ‘j’ at time ‘t’
\( k \in \{1 \text{ to } m\} \) where \( m = \text{number of ants} \)
\( \eta_{ij} = \text{correlation between the user i and j} \)
\( \alpha, \beta = \text{The parameters controlling the significance of the visibility ant trail respectively.} \)
Step 6: After the complete return of ants after the new birth, the best tourism choice and the pheromone path improved.
Step 7: If the breakdown occurs, the round ends, the other tabu list is empty and the cycle continues from Step 2.

2. H-TDMA (Hybrid Time Division Multiple Access) and H-TCMR (Hybrid Trust Cluster based Multiple Routing)

H-TDMA is a combination of time-division multiple access (H-TDMA) and the Unifying Slot Assignment Protocol (USAP). When a mobile block enters the network in USAP, it's not really assigned a y slot and has no knowledge about everyone's neighbours. The new node then chooses an open slot and assigns it to itself. Finally, the new node tells its neighbours of the slot that has been chosen. Hybrid Trust Cluster based Multiple Routing (H-TCMR) tends to reduce the amount of messages received within the network, reducing the network's overall energy usage. In this type of network Resource allocation plays an important role to minimize the features of network such as time, cost, energy, etc. This work mainly focus on time ie., by allotting time slot for each node, the transmission of data will be fast and secure. So, H-TDMA is used for allotting time slot for each node along with this USAP protocol is also used. This protocol is used to determine whether a node is allocated or uninitialized in a network. The data is transmitted via neighbour nodes, which are thought to be at risk.

3. ABT (Adaptive Booting Technique)

MANET is represented by a graphical model \( G = (V, E) \), in which ‘V’ denotes the amount of MNs \( mn_1, mn_2, \ldots, mn_n \) that are located in a squared region of ‘N * N’, and
‘E’ denotes MN contact. The suggested technique uses the ABT approach to assess the trustworthy node based on three characteristics: cooperativeness \( C_v \), residual energy of the node \( E_r \), and context of the mobile node \( m_n \). As a consequence, data transmission is routed through the reliable node, improving Qos metrics such as PDR as well as reducing E2E delay between sender as well as receiver.

Simulation Result

The proposed SRTE system's main goal is to increase security execution in the MANET by better Qos measurements. The NS2.35 simulator is used to simulate the SRTE process and current techniques. The Random Waypoint mobility model is used to generate the output. The running time is defined in seconds. To identify the confided node for secure transmission, the DSR routing protocol is used. In this section, the effects of the SRTE framework as well as current models such as DTN (Singh, 2017) and the multidimensional confidence model (Ali, S.S, 2017) are discussed and compared. Different Qos constraints such as Energy, Average Delay, Throughput, Routing overhead, Overall Cluster Efficiency, as well as Packet Delivery Ratio (PDR) with the amount of MN as well as DP are used to control the action of the SRTE system. Tables as well as graphical results are used to do the simulation research.

1. Energy and Average Delay

The power to work is referred to as energy. The word "energy conservation" refers to the use of less energy to produce the same amount of energy. The cumulative amount of energy expended when sending and receiving data is referred to as energy consumption. During packet transmission, a node expends a certain amount of energy. Delay relates to the process of allowing data transfer to be interrupted. A network's architecture and output characteristics include network latency.

\[
RQ = \frac{\text{min}, \text{ttl} \times \text{min}, \text{energy}}{\text{Hopcount}}
\]

\[
\text{Average Delay} = \frac{\text{Sum of all packets Delay}}{\text{Total No.of Received Packets}}
\]

As previously mentioned, the average delay is done by calculating the delays for each mobile node sent from the total number of detected packets. In addition to the obtained controlling data packet, the submitted data packet is calculated using node models based on the delay factor of the actual node power.
2. Throughput and Routing Overhead

In most cases, throughput is expressed as an average and computed in bits per second (bps). Because of the high rate of failed message transmission, throughput is reduced. The level of efficient packet distribution from one network point to another is determined by throughput. The sum of data successfully transmitted from one node to another in a given time span is known as throughput. \( Dp \) represents the number of submitted packets, as well as \( Ps \) represents the size of a packet in Eq (5) throughput. Packet bandwidth is the amount of time it takes to send data across a network. Each package includes extra bytes of data as well as a control packet applied to the transmitted data to carry out the related data's routing information, error correction, including operating instructions.

\[
\text{Throughput} = \frac{D_p \times P_s}{\text{Total Number of Internal Data packets Received}} \tag{5}
\]

\[
\text{Overhead} = \frac{\text{Data packets Received}}{\text{Control packets generated}} \tag{6}
\]

3. Packet Delivery Ratio and Overall Cluster Performance

PDR refers to the ratio of packets transmitted by the source node to packets received by the destination node. PDR is expressed as the ratio of easily determine to destination as a percentage of the total number of packets sent out by the sender. The ratio is a type of packets sent divide by the number of packets received.

\[
\text{Packet delivery ratio} = \frac{\text{Received Packets}}{\text{Send packets}} \times 100 \tag{7}
\]

In figure 2 (a) describes the performance analysis of existing TCMR and proposed system Hybrid Trust Cluster based Multiple Routing. Here the research work will produced trustworthiness and healthy data transmissions in MANET environment. Here evaluate the parameters compared with existing system, such as Energy, Delay, Packet delivery ratio, Routing overhead. In figure 2 (b) describes the performance analysis of existing methods and proposed system. Here the research work will produced security, trustworthiness, strong node calculation and healthy data transmissions in MANET environment. In this section, compare the parameters to the existing system, such as ZRP, IWD, RA, DTN, and SRTE. In terms of Energy, Average Delay, Packet Delivery Ratio, Routing Overhead, and Throughput, SRTE produces the best results. So the proposed system is healthy and trustworthiness of the data transmission to source and designation in the mobility environment.
Conclusion

A novel approach in MANETs, SRTE is suggested for QoS-aware encrypted data communication. The QoS has been improved by using attribute analysis to find the trusted MN. MN's confidence measure represents node activity in real time and assesses MN's trustworthiness. For efficient correspondence, the MN is chosen based on its trustworthiness. The H-ACO-DSR is used for safe data communication, followed by HTDMA and HTCMR to boost device reliability, cluster performance, and trustworthiness, and finally the ABT approach is used to identify the strong nodes as trustworthy or malicious. The good classification results improve the confidence assessment accuracy, which leads to better QoS metrics in MANET. When compared to traditional approaches, the efficiency findings show that the SRTE technique offers higher PDR with lower time in Energy, Average Delay, Routing overhead, and Throughput.

Acknowledgement

This research was funded by Dr. S.H. Krishnaveni, Associate Professor, Department of Computer Science and Engineering, Mathews II College of Engineering, sasthamcotta, kollam. Friends who assisted with (MANET's) and moderated this text, which significantly improved the manuscript, are also grateful.

References


