Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2088289, 9 pages
https://doi.org/10.1155/2022/2088289

Research Article

Execution of Multitarget Node Selection Scheme for Target Position Alteration Monitoring in MANET

Nookala Venu,[1] **D. Yuvaraj**,[2] **J. Barnabas Paul Glady**,[3] **Omkar Pattnaik**,[4] **Gurpreet Singh**,[5] **Mahesh Singh**,[6] **and Amsalu Gosu Adigo**[7]

[1] *Post-Doctoral Research Scholar, Department of Electronics & Communication Engineering, Srinivas University, Mangalore, India & Professor, Department of Electronics & Communication Engineering, Balaji Institute of Technology & Science, Warangal, India*
[2] *Department of Computer Science, Cihan University-Duhok, Kurdistan Region 42001, Iraq*
[3] *Department of Electrical and Electronics Engineering, Sathyabama Institute of Science and Technology, Chennai, 600119 Tamil Nadu, India*
[4] *Department of Computer Science Engineering, Govt. College of Engineering, Keonjhar, Odisha, India*
[5] *Department of Computer Science and Engineering, Department of Computer Science Engineering, Punjab Institute of Technology, Rajpura (MRSPTU Bathinda), Rajpura, Punjab 140401, India*
[6] *Department of Electrical and Electronics Engineering, Shri Shankaracharya Technical Campus, Durg, Bhilai, Chhattisgarh 490020, India*
[7] *Center of Excellence for Bioprocess and Biotechnology, Department of Chemical Engineering, College of Biological and Chemical Engineering, Addis Ababa Science and Technology University, Ethiopia*

Correspondence should be addressed to Nookala Venu; nookalavenu11@gmail.com
and Amsalu Gosu Adigo; amsalu.gosu@aastu.edu.et

Received 28 February 2022; Revised 28 April 2022; Accepted 3 May 2022; Published 8 June 2022

Academic Editor: Mohammad Farukh Hashmi

In mobile network, nodes are normally placed in some locations after travelling with various speeds to another location. Packets were broadcast to some location receiver node, but they are moved to another location, due to that node is not able to receive those packets. Attacker node present in routing path should accept those packets, and it acts as original node. Communication privacy is reduced for mobile network. It improves the communication overhead and end to end delay. So, the proposed Enhanced Packet Acceptance for Target Position Alteration (EPATP) technique exactly monitors the target node position, depending on the position to assign the relay node for packet forwarding from sender to target node. Multiaccepter Assigning Algorithm is designed, and if any target node should not receive those packets, it provides another chance for packet receiving by next target node, and it assigns multiple target node for accuracte communication. It reduces communication overhead and end to end delay.

1. Introduction

Mobile nodes are independent in the network environment and should be used in military and business parts for processing, to estimate the repetitive else unsafe for nodes. The network contains mainly difficult packet transmission needs. Packet sharing is important for the incomplete process of the network environment [1]. The group requires a regular network to manage packet transmission, and consequential in recurrent path alters based on the speed of mobile nodes. This topology production process is used to provide a diversity of mobile ad hoc network routing techniques. The mobile network is active, identity processing, and communication ever groups of mobile nodes. It is normally produced by a particular process [2].

All nodes within a mobile network are called a node and should take the position of a target node with an intermediate node. Message crossways of the system are achieved and obtained by data packet broadcasting to a target node. While a sender to target nodes, traight connection is occupied by intermediate nodes which are used for forwarding data packets [3]. Mobile node sharing packets are through usual wireless. Wireless communication can be insignificantly interrupted by some attacker nodes in a range of the sender node. It should go away from mobile network free to a range of intrusion like dropping attack and data blockage attack. It should cooperate the reliability of the network infrastructure [4].

Data dropping during the packet transmission time may provide an intruder with the resources to cooperate with the reliability of a network environment. It is obtained from the influence routing table for data storage, injecting fake path for packet transmission else altering paths. MitM attack should be introduced to influence communicating packet and to forward a data packet through attacker nodes [5]. The protected communication technique is present to alleviate intrusion over mobile network, except those do not expand protection to the previous data packet. Independent network needs an important quantity of packet sharing.

Issues resolving techniques like a disseminated process data sharing are necessary to resolve process preparation problems without node intrusion [6]. The output of the scheme is susceptible to packet drop and wrong packet transmission; incomplete data packet should guide to secondary best else unsuccessful process allotments. Previous option for communicating to multi-instantiated target node contains listing-based result that is additionally elastic, which considers the collection conditional coefficient to organize since they do not need alterations to the fundamental technique [7]. Directory-based communication depending outputs contain the problem of not identifying the position of the target node except the position of the target node resolution. Furthermore, the entire presentation of the directory depending method is increased by containing well-organized network protocol multicast method [8].

Organismic self-configured and self-prepared like a network setup with deployment is very easy in any network environment. This network finds its main utilization in case of an urgent condition to make easy and successful packet transmission in failure revival process, while regular environment depends on packet transmission which is render broken [9]. Many hop methods make easy data broadcasting in a mobile network anywhere; many relay nodes should broadcast the packets from the sender node to the target node. For that, networks must not jump to any objective environment, and some nodes have the authorized connection; travel also departs the mobile network at some indications of time period creation of them defenseless and accountable to different intruders. Pertaining to the deficiency of a middle ability management, the organization of the whole system be fall on all nodes connected with each other [10].

Residual of the paper is designed as follows. Section 2 provides related works. Section 3 presents the details of the proposed Enhanced Packet Acceptance for Target Position Alteration (EPATP) technique which achieves an accurate data transmission among mobile nodes, and the best routing path is obtained. Section 4 provides simulation performance result analysis obtained under various metrics. Section 5 concludes the paper with future direction.

2. Related Works

Awatade et al. [11] present mobile network nodes are fixed else dispersed in ad hoc network, and they are broadcast data packets using wireless medium. Protection is calculated quiet in mobile network environment since mobile network contains the wide allocation of node and open intermediate, and it becomes susceptible to intruder very quick. To suggest and perform more authoritative and protected attack identification scheme is known as enhanced EAACK constructed for mobile network. This technique uses techniques like a fusion cryptography with an active hypothesis for minimizing communication overhead and eliminating discarded node and broadcast overload data packet among specific positions. The experiment is evaluated by using metrics transmission rate and communication overhead.

Shetty [12] proposes to examine one of the intrusions which is called the black hole intrusion. This node is a misbehaving node forwards a fake path through itself as the most compressed and suitable route to the target node. That made-up path is the hateful node technique to interrupt and put away all data packets planned for the target node. The method utilizes secure ad hoc on demand distance vector communication method which is used to the promoter in this network, to disclose and interrupt black hole intrusion in a mobile environment. Watchdog technique as an add-on in ad hoc network communication scheme is used for malicious node finding and removing from the network. The present technique should improve the transmission rate and presentation in the attendance of many attacker nodes in a network environment.

Sangeetha and Sathappan [13] proposed novel optimization technique for given that protected data delivery is known as identity planned B+ hierarchy Indexed Key in Mobile network. In particular, it depends on the occurrence of mobile node operation, and B+ hierarchy organization is created anywhere; all nodes have only keys, provided that privacy of the broadcasted data packet. Specify the data packet to be broadcast, and a recent scheme for resourceful broadcast to the next intermediate node is available. In the calculation, an identity category key is created in that sender node broadcasts the protected data packet to the target mobile node. At last, indexing is complete to create a self-organized key to increase right of entry time of relay nodes for packet broadcasting. Experimental output depends on authentic traces with many time slots for diverse mobile node thickness and velocity express of the efficiency of the technique.

Sharma et al. [14] propose security depending communication technique to calculate honesty of the route earlier than it is chosen for data transmission. Unambiguous route secures calculation with a trustworthy node, through among suggestions from next intermediate nodes through the route, guarantee the route allocation as secure. The output present is to make the mobile network secure from packet loss for intrusion occurrence and its variant such as energetic fake with energy usage intrusion. For detailed about communication technique on the foundation of protection by keeping away from and identify wormhole intrusion. The wormhole intrusion is made on the network layer, and it is solitary of the harsh intrusion in a wireless mobile network environment. The wormhole intrusion is misbehaving nodes forever to provide a delusion to both point source and target points.

Airehrour et al. [15] propose ranking secure technique which is a safe routing procedure for the mobile network that should depend on the security level of network nodes in the environment. It uses security to separate intrusion routing that provides protected communication of data packet overload and also increases the transmission rate. The experimental output contains the security cooperation, and the transmission rate is efficient in present ranking secure technique to distinguish with conventional routing procedure.

Song et al.,[16] propose protection and well-organized communication by leveraging data packets in planned border mobile network environment. The present technique exploits concurrent data packet transmission. Except for message, it is also to make easy many points to transmit node choosing path detection provided that equally concurrent data transmit with unicast forces. In the present, scheme transmission is familiar which is carried out only by multipoint relaying nodes that should minimize bandwidth consumption is distinguished to uncontaminated dropping techniques like a Multicast Ad hoc On-Demand Distance Vector communication. Additionally, by keeping away together from broadcasting of detailed construction of broadcasting data packets in the network also improves many points to transmit the chosen technique which depends on an inclusive scheme by enabling the joint total message.

Selvigrija and Premkumar [17] present a technique which offers faultless data delivery in a mobile network regardless of its intimidation using chance cast and the previous technique such as dual hop reply packet else sender concentrating reply packet must not grasp, while a network topology alters regularly else while a node cooperates. Those demerits are to be indicated to ensure protected linking nodes between sender and the target nodes. The sender node crash contact to susceptibility is also reduced by applying this technique. Present and optimize result for exceeding issues using faultless data delivery method that overcomes eaves dropping depends on reply packet from the relay node.

Tan et al. [18] propose a technique which offers protected path detection for the ad hoc routing in direct to avoid black hole intrusion. This technique needs the sender node and the target node to confirm the series numbers in the path request and path reply packet correspondingly, depends on distinct threshold previous to establish a link with a target node for broadcasting data packets. The experimental output shows an increased transmission rate in various network infrastructures using present technique is distinguished with model AODV procedure.

Hurley-Smith et al. [19] proposed protected communication and message safety method is constructed to obtain full entire security. The utilizing of packet transmission protection technique is created for wireline, and WiFi networks should fix a serious load on the incomplete network energy of a mobile environment. It indicates the problems, to overcome and use a novel secure structure. This structure is constructed to permit the previous network with communication scheme to execute their process, while provided that node security, the right of entry manage, and packet transmission protection technique. It presents a novel security structure for the mobile network. The experimental output indicates comparison of the present method is better protection than existing methods.

Garcia-Luna-Aceves [20] proposed many cases of target communication uses simply space details to many instantiated targets; lacking senders contain to create transfer, identify the network technique, use whole routes to target case, and else distinguish regarding each case of the target node. It is used in name-based contented communication, IP single cast communication, and multicast communication, smooth in conditions where the network technique is extremely active in the condition of the mobile network. This is indicated in that many cases of target communication provide numerous round free paths to the target. Widespread experiments execute in the situation of mobile network present method is better than unicast method.

As we know the network that has the mobile nodes sometimes is unstable that may also does not maintain the accuracy of data. In order to rectify the proposed method called enhanced data, accuracy-based path discovery is introduced to receive the data in which accuracy rate is so high. Further, it can detect congestion and energy consumption, and size is reduced [21].

Here we have introduced a security system that is a trust-based protocol which depends on the Mac layer method which reaches the confidentiality and authentication of packets. It has packets in routing layer and MANET that have link layer. The delivery percentage of packets is increased when a low delay occurs, and speed is high [22].

Here we initiated to create an enhanced distributed certificate authority scheme in the motive to give away the data of high integrity. While doing so, the network we use becomes more secure inwards and also outwards. The results show more packet delivery when low delay and overhead occur [23].

3. Overview of Proposed Scheme

The unstable mobile nodes are generally located in particular position, subsequent to the node passes through with different velocities to another location in network environment. Packets were broadcast to some location receiver node, except they are travelled to various position, which are not ready to accept particular data packets [24]. The intruders are available in communication path, it provides the advertising packet, and packet has information such as this is target node, so it is ready to accept data packet in current position. Using data packets, attacker should hack the various information and misuse it. It makes the poor communication privacy in mobile environment. It increases the communication overhead and also end to end delay.

So, the proposed Enhanced Packet Acceptance for Target Position Alteration (EPATP) method is used to accurately observe the target node location. The sender node must track every relay node position; after that, select the relay node for packet forwarding from sender to target node in mobile network environment. The Multiaccepter Assigning Algorithm is constructed, whether the target node must not accept those packets from relay, because target node is in and out of coverage area; then, it provides an additional chance for packet accepting by next target node; it allocates the multiple target node for high accuracy of packet transmission. It minimizes the communication overhead and reduces packet latency.

Figure 1 shows block diagram of Enhanced Packet Acceptance for Target Position Alteration Technique. Subsequently, mobile nodes are travelling along network environment. Sender broadcast data packet to target node through relay nodes. Enhanced Packet Acceptance for Target Position Alteration technique is used to obtain accurately and observe the target node location details. To check target node within coverage, choose it; otherwise, choose another target node. Multiaccepter Assigning Algorithm is designed to get minimum overhead and end to end delay.

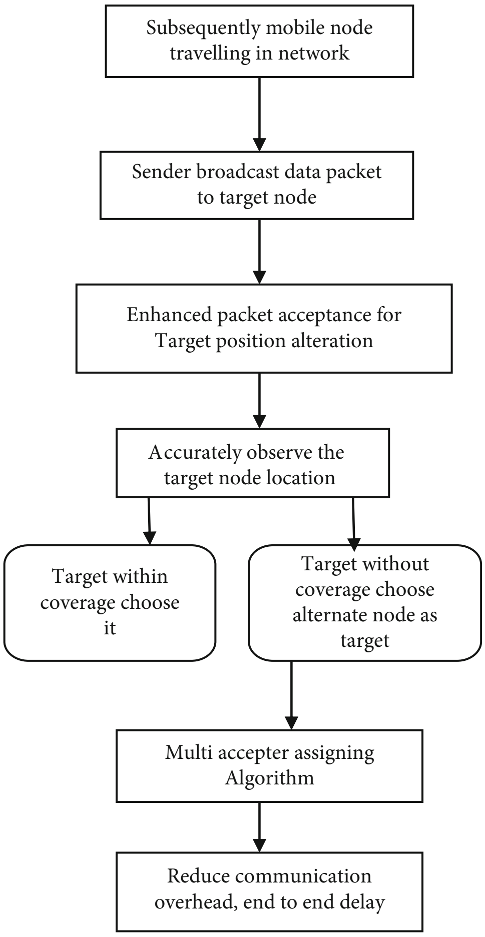

Subsequently mobile node travelling in network
Sender broadcast data packet to target node
Enhanced packet acceptance for Target position alteration
Accurately observe the target node location
Target within coverage choose it
Target without coverage choose alternate node as target
Multi accepter assigning Algorithm
Reduce communication overhead, end to end delay

Figure 1: Block diagram of Enhanced Packet Acceptance for Target Position Alteration Technique.

3.1. Subsequent Mobile Node Travelling in Network. Mobile network nodes are placed in a multidimensional environment; also, the position of every node is tracked; it works to move within the network infrastructure and accuse the mobile node capacity. Nodes initiate its travel from home place; it moves along a designed route in the coverage area and also takings to the provision place at the finishing stage of its node movement, whereas on its route, the path establishment provides an amount of relay nodes available in routing path. Consider that the network nodes have enough quantity of energy to hold node movement, packet aggregation, and energy move to mobile nodes previous to it proceeds to the provision stage, where Mn is mobile node, US(Mov) is unstable movement, and Com is communication.

$$\mathrm{Mn} = \mathrm{US(Mov)} + \mathrm{Com}. \tag{1}$$

The exhaustive energy recharging scheme is included because node travels take more energy, so recharge it before performing packet transmission. We already allocated the packet travelling relay node in communication route and the whole quantity of time instance used for the path establishment along mobile node travelling in network environment [25, 26]. The whole mobile node moving time is the length of the allocated route; also, track the distance between sender node and target node in routing path. Velocity of the each node is different; then, it is important for assigning relay on current position in network environment. The vacation time τvac that indicates the quantity of time instance was used to broadcast data packet from sender through updated relay to target node. The whole time slot is beside the allocated routing path. Ip ∗ Cp is initial and current position.

$$\mathrm{US(Mov)} = \mathrm{Ip} * \mathrm{Cp} - \tag{2}$$

Path establishment is also portioned as a mobile environment for the target node. Consequently, the target node is mobile when it operates as the end node for all data collected from the mobile nodes in the network infrastructure. To consider a stable data making rate from all mobile nodes, then communicate concurrently as data are transferred to the mobile target node. Towards preserving energy, multihop data broadcasting is placed through the mobile nodes. In a mobile node, consider that the communication action is the leading sender of the node's energy usage. Consider a mobile node has its energy control ability for that all nodes can alter its communication energy range depending on its space to the target node in the network. It makes some inferences of the location of target node in difficult to track in normal routing [27]. The energy usage rate for broadcasting one unit of data transmission is from source node to target node. S is speed.

$$\begin{aligned} \mathrm{Ip} &= \frac{Ix}{Iy} * S, \\ \mathrm{Cp} &= \frac{Cx}{Cy} * S. \end{aligned} \tag{3}$$

The quantity of energy used at node current position during communication time is the highest potential quantity of energy used at packet acceptance by the next node in a routing sequence. Authentic quantity of energy usage for sender node in the initial stage should be minimum than the packet accepted by target node energy usage [28]. Establish path to order the relay node based on distances between sender and target nodes, secure identifiers, and succession count is fashioned by the target node. As an alternative of identification, the most new series digit for an available target node, a sender having the series count should be generated by the target at present report by its relay node. Details of target node are maintained in routing table.

3.2. Enhanced Packet Acceptance for Target Position Alteration. For that condition target node is external in the whole network coverage area, the mobile nodes participate in the network. By storing the details on the relay node identity of the target node, the mobile node attempts to increase the request message to an utmost of areas further than arrival at mobile nodes. Extend the request message to multiple target node, at all communication with a next relay node on the path and in a continuous mode. It is easy and effectual for some conditions, except it is based on the thickness and speed of the node traffic in the coverage area. For particular condition, the broadcasted data packet rate is maximum and also origin considerable path failure, consequently latency for the monitoring process, and also the localization of the target node. The unstable mobile node position should reduce the amount of data packets exchanged among mobile nodes to ensure the best answer instance.

$$\mathrm{US}(\mathrm{Mov}) = \left(\frac{Ix}{Iy} * S\right) * \left(\frac{Cx}{Cy} * S\right). \tag{4}$$

Furthermore, consequently, at the mobile nodes, every node identity is encapsulate in a communication with an exclusive consecutive digit to differentiate various packet loss incidents. At first, it is a common design on the situation of the targeted node. It is essential to monitor the vehicle node of the middle relay node to forward a request message packet to each mobile nodes present in coverage range. The request message is summarized in a data packet having a lesser quantity of data like mobile node identity and location. All data packet is recognized by an exclusive sequential amount relating a specific mobile node at an exact point. Subsequently, for the acceptance of this request message, the mobile node transmits data packets within coverage limit target node. Otherwise, target node is without coverage limit, and mobile nodes accept the query from sender and reply the correct answer to source node.

$$\mathrm{US}(\mathrm{Mov}) = \left(\frac{Ix}{Iy} * \frac{Cx}{Cy}\right) * S^2. \tag{5}$$

Sequence to minimize the traffic, mobile nodes do not retransmit the request in the mobile node coverage limit. Mobile nodes are detected whether it is in coverage area condition or it accepts a request from the mobile nodes else by asking its local plan. Subsequently, for the receiving of a request message, all mobile nodes monitor the details restricted in the message packet and also distinguish its individual node identity with the individual restricted the message packet. Condition there is an equivalent that indicates the target node is tracked. In addition, the sender node transmits a request packet. By enchanting into the description the information of map of the coverage limit at all mobile nodes, it can decide the location of the nearest mobile nodes, significant to facilitate its location which is permanent; also, it is experimental on the plan. Normally, mobile nodes should go behind routes strong-minded by the network environment, and mobile nodes travelling in the similar way and are subsequent to a frequent route have well-built possibility to stay near when crossing of a routing path.

$$\begin{gathered}\mathrm{Com} = \mathrm{SeqTransmission} + \mathrm{time}, \\ \mathrm{SeqTransmission} + \mathrm{time} = \mathrm{accuracy}.\end{gathered} \tag{6}$$

It should be extraefficient in conditions of data packets to employ many mobile nodes to broadcast the recurring data packets shown in Algorithm 1. It should minimize the quantity of packets and also evaluate the traffic rate. The efficient method to distribute packets in a MANET is by allocating relay node to the additional mobile node in the communication limit of the broadcaster. While the target node should transmit a reply packet, all nodes in its extent accept data packets. All mobile nodes estimate the broadcasting time between target and the sender nodes. The mobile node having the communication time set in a distinct time retransmits the data packets in turn and continuously. The gap of broadcasting time is recognized by all mobile nodes.

3.3. Multiaccepter Assigning Algorithm. Time gap with the information of the efficient coverage area and the communication time to directly, at the ending of the efficient limit is identified. The reply packet has details on the localization that the target node is established. It is probable by using a position network like mobile target node. It should avoid request and reply packets from broadcast considerably, as time counter control is applied for all data packets. In addition to minimize attacks, a back-off technique is old. The reverse off time is based on the thickness of the modern coverage range. The dispensation executes by the mobile nodes are within coverage limit. It is used for relying data packets in routing path. Otherwise, mobile nodes are out of coverage limit. The alternate relay node is selected to perform packet transmission.

$$\begin{gathered}\mathrm{Com} = \mathrm{accuracy}, \\ \mathrm{Mn} = \left(\frac{Ix}{Iy} * \frac{Cx}{Cy}\right) * S^2 + \mathrm{accuracy}.\end{gathered} \tag{7}$$

```
Step1: Track the relay node position.
Step 2:For each sender nodeestablish communication path
Step3:Target node update location
Step 4: Identify current position of target node
Step 5: if {attacker==available}
Step 6: Advertisement packet is broadcasted
Step 7: else
Step 8: if {attacker==not available}
Step 9: It does not provide advertisement packet
Step 10: It broadcast request packet to target node
Step 11: Target node within coverage accept it, otherwise alternate target is used
Step 12: end if
Step 13: end for
```

Algorithm 1: Enhanced Packet Acceptance for Target Position Alteration.

Multiple target node is deployed in network environment. If any of the target node should attempt to fail for packet transmission, it assigns next target node for receiving those data packets. If any attacker node is available in routing path, they are moved to out of coverage range, since its energy capacity is reduced to reach minimum level. It increases the packet transmission rate, because it chooses only maximum energy node for communication. It establishes the sequence routing from sender to target node.

In Algorithm 2, multiple accepter is a multiple target node allocation method, and it allocates the many target nodes for receiving data packets in movable mobile network. It allocates the intermediate nodes are trusty node, and its delivery ratio is individually higher one. It reduces communication overhead and end to end delay.

Packet ID: packet ID contains each mobile node detail. It also achieves the exact location of many relay nodes in routing path designing in network infrastructure.

In Table 1, the proposed EPATP packet format is shown. Here, for the source and destination node ID field, each carries 4 bytes. Third one is subsequent mobile node travelling in network occupies 3 bytes. Mobile nodes are move along network in a subsequent manner, and the travelling location of mobile node details is tracked and stored in routing table. In fourth field, it occupies 4 bytes. For Enhanced Packet Acceptance for Target Position Alteration, it increases the packet transmission, because target node position is accurately monitored, so it receives the data packets successfully. In fifth, it occupies 5 bytes. Accurately observe the target node location; this scheme analyzes node location within or without coverage area; after that, within coverage area means assigning communication else not assigning communication. Multiaccepter Assigning Algorithm occupies 3 bytes, and it uses many target nodes; if anyone failed to receive, it means use another one for communication.

```
Step 1: Establish Many Target node.
Step 2: for each search advertising attacker node.
Step 3: if {lowaccuracy==unsecure}
Step 4: identify attacker node
Step 5: Deny the communication on that node
Step 6: else
Step 7: if {high accuracy==secure}.
Step 8: use that node to transmit data packets sequencially.
Step 9: End if.
Step 10: End for
```

Algorithm 2: Multiaccepter Assigning.

4. Performance Evaluation

4.1. Simulation Model and Parameters. The proposed Enhanced Packet Acceptance for Target Position Alteration (EPATP) method is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 wireless ad hoc nodes are placed in a 1020 meter × 1020 meter square region for 30-millisecond simulation time. Each mobile node goes random manner among the networks in different speeds. All nodes have the same transmission range of 250 meters. CBR Constant Bit Rate provides a constant speed of packet transmission in network to limit the traffic rate. DSDV destination sequence distance vector routing protocol is applied to achieve higher accuracy for data transmission along movable mobile nodes. Table 2 shows simulation setup estimation.

Simulation result: Figure 2 shows that the proposed EPATP technique is used to achieve higher accuracy for packet transmission compared with existing SPM [16] and RMI [20]. EPATP contains tracks of every relay node location, and it should maintain those details in routing table. Multiaccepter Assigning Algorithm is designed to get alternate target node for receiving data packets. It reduces communication overhead and reduces end to end delay.

4.2. Performance Analysis. Simulation to analyzing the following performance metrics using X graph in NS 2.34 is as follows:

End to end delay: Figure 3 shows end to end delay is estimated by amount of time used for packet transmission from source node to destination node. Multiaccepter Assigning

Table 1: Proposed EPATP packet format.

Source ID	Destination ID	Subsequent mobile node travelling in network	Enhanced Packet Acceptance for Target Position Alteration	Accurately observe the target node location	Multiaccepter Assigning Algorithm
4	4	3	4	5	3

Table 2: Simulation setup.

No. of nodes	100
Area size	1020 × 1020
Mac	802.11 g
Radio range	250 m
Simulation time	18 ms
Traffic source	CBR
Packet size	512 bytes
Mobility model	Random way point
Protocol	DSDV

Algorithm is designed to get higher transmission rate. In the proposed EPATP method, end to end delay is reduced compared to existing methods SPM and RMI.

$$\text{Endtoenddelay} = \text{endtime} - \text{starttime}. \tag{8}$$

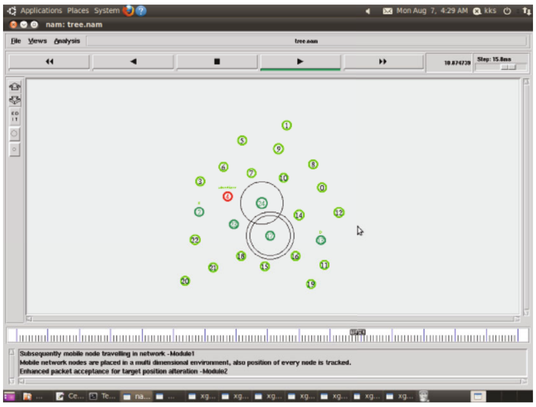
Communication overhead: Figure 4 shows communication overhead is minimized in which sender transmits packet to receiver node. Multiaccepter Assigning Algorithm does not permit to rebroadcast data packets; it provides higher accuracy of communication among mobile nodes. In the proposed EPATP method, network overhead is minimized compared to existing methods SPM and RMI.

$$\text{Communicationoverhead} = \left(\frac{\text{numberofpacketlosses}}{\text{received}}\right) * 100. \tag{9}$$

Packet delivery ratio: Figure 5 shows packet delivery ratio is measured by no. of received from no. of packet sent in particular speed. Node velocity is not a constant, and simulation mobility is fixed at 100 bps. In the proposed EPATP method, packet delivery ratio is improved compared to existing methods SPM and RMI.

$$\text{Packetdeliveryratio} = () * \text{speed}. \tag{10}$$

Detection efficiency: Figure 6 shows detection efficiency, attacks are occurred, and packet transmission is repeated from source node to destination node. Time was spent to detect the intruders. In the proposed EPATP method,



Subsequently mobile node travelling in network -Module1
Mobile network nodes are placed in a multi dimensional environment, also position of every node is tracked.
Enhanced packet acceptance for target position alteration -Module2

Figure 2: Proposed EPATP result.

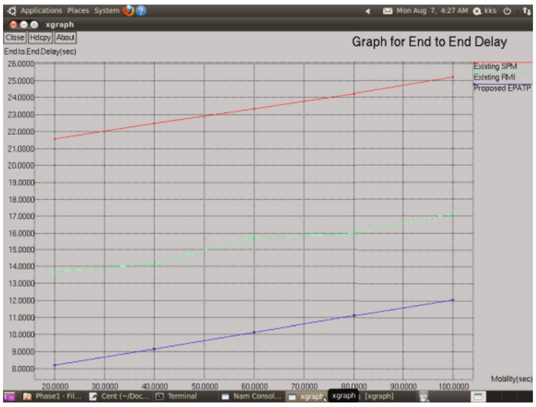


Figure 3: Graph for mobility vs. end to end delay.

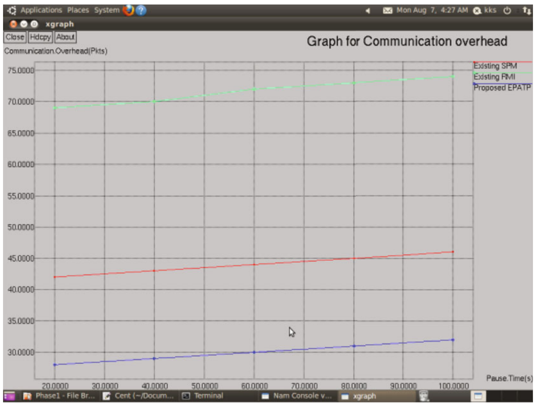


Figure 4: Graph for pause time vs. communication overhead.

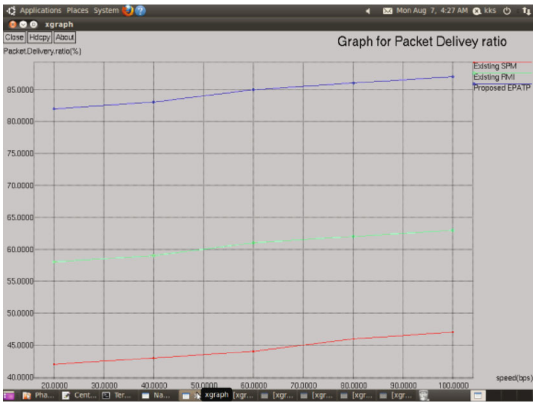


Figure 5: Graph for nodes vs. packet delivery ratio.

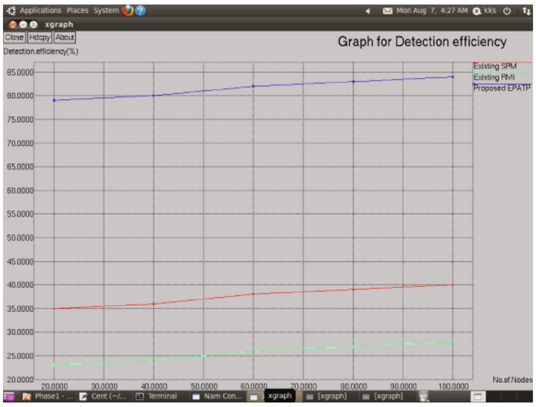


Figure 6: Graph for nodes vs. detection efficiency.

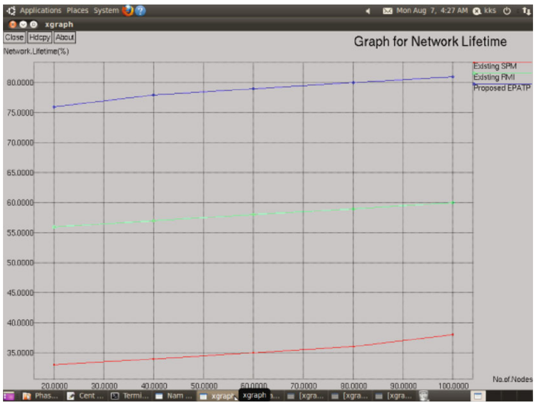


Figure 7: Graph for nodes vs. network lifetime.

detection efficiency is improved compared to existing methods SPM and RMI.

$$\text{Detectionefficiency} = \frac{\text{attackdetectionrate}}{\text{overalltime}}. \tag{11}$$

Network lifetime: Figure 7 shows that lifetime of the network is measured by node process time taken to utilize network from overall network ability; it has Multiaccepter Assigning Algorithm to achieve alternate target node, if any target node gets failed. In the proposed EPATP method, network lifetime is increased compared to existing methods SPM and RMI.

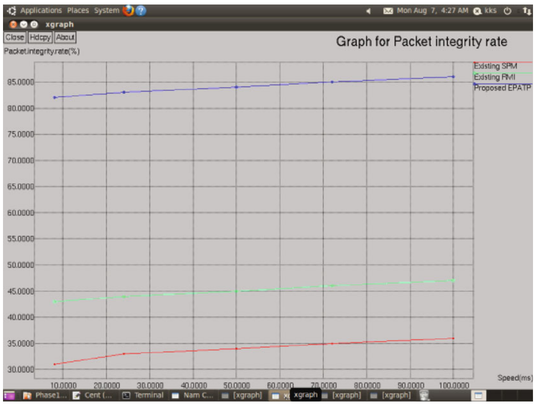


Figure 8: Graph for speed vs. packet integrity rate.

$$\text{Networklifetime} = \frac{\text{timetakentoutilizenetwork}}{\text{overallability}}. \tag{12}$$

Packet integrity rate: Figure 8 shows that packet integrity of particular communication in network is estimated by nodes transmit packet with coverage limit. In the proposed EPATP method, packet integrity rate is improved compared to existing methods SPM and RMI.

$$\text{Packetintegrityrate} = \left(\frac{\text{numberofpacket successfully sent}}{\text{coverage limit}}\right) * 100. \tag{13}$$

5. Conclusion

Movable mobile nodes are deployed in network environment. If sender node starts to broadcast data packets to target node, target node position is every time changed, so the intermediate node acts as target node is known as attacker node. It broadcasts the advertisement packet to any other node within coverage limit that packets have details such as ready to transmit and receive data packets. It increases communication overhead and end to end delay. So, the Proposed Enhanced Packet Acceptance for Target Position Alteration (EPATP) technique is used to achieve higher accuracy for data packet transmission from sender node to target node. It verifies the target node coverage limit, and within limit means choose for communication; otherwise, without limit means not allowed to perform communication. Multiaccepter Assigning Algorithm is designed to provide many target nodes to accept the data packet, and if anyone gets failure, use alternate target node. It minimizes communication overhead and end to end delay. In future work, focus on uncertain misplacing node identification to analyze various parameters.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

There is no conflict of interest.

References

[1] P. S. Kiran, "Protocol architecture for mobile ad hoc networks," in *2009 IEEE International Advance ComputingConference (IACC 2009)*, 2009.

[2] A. Chandra, *Ontology for Manet Security Threats*, PROC. NCON, Krishnankoil, Tamil Nadu, 2005.

[3] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," *International Journal of Computer Scienceand Security*, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle, "A cluster-based approach to consensus based distributed task allocation," in *Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd EuromicroInternational Conference on*, pp. 428–431, IEEE, 2014.

[5] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation design," in *Distributed Computing Systems Workshops, 2004. Proceedings. 24thInternational Conference on*, pp. 698–703, IEEE, 2004.

[6] T. Clausen, P. Jacquet, C. Adjih et al., *Optimizedlink State Routing Protocol (OLSR)*, IEEE EXPOLRE, 2003.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, vol. 2, pp. 249–256, IEEE, 2007.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," in *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*, pp. 317–321, IEEE, 2011.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE wireless communications*, vol. 11, no. 1, pp. 38–47, 2004.

[10] N. Garg and R. Mahapatra, "MANET security issues," *IJCSNS*, vol. 9, no. 8, p. 241, 2009.

[11] S. Awatade and S. Joshi, "Improved EAACK: develop secure intrusion detection system for MANETs using hybrid cryptography," in *Computing Communication Control and automation (ICCUBEA), 2016 International Conference on*IEEE.

[12] N. P. Shetty, "Interception of black-hole attacks in mobile adhoc networks," in *Inventive Computation technologies (ICICT), International Conference on*, vol. 3IEEE.

[13] S. Sangeetha and S. Sathappan, "Securing data retrieval based on tree indexed self organized key in mobile ad-hoc network," in *Computation System and Information Technology for Sustainable Solutions (CSITSS), International Conference on*IEEE.

[14] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: wormhole detection and prevention," in *Computing, Communication and Automation (ICCCA), 2016 International Conference on*IEEE.

[15] D. Airehrour, J. Gutierrez, and S. K. Ray, "GradeTrust: a secure trust based routing protocol for MANETs," in *Telecommunication Networks and Applications Conference (ITNAC), 2015 International*IEEE.

[16] R. Song, J. D. Brown, H. Tang, and M. Salmanian, "Secure and efficient routing by leveraging situational awareness messages in tactical edge networks," in *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*IEEE.

[17] P. Selvigrija and J. Premkumar, "Bandwidth shared acknowledgment (BSA)—a secure intrusion detection and multi path routing for MANETs," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*IEEE.

[18] S. Tan and K. Kim, "Secure route discovery for preventing black hole attacks on AODV-based MANETs," in *ICT Convergence (ICTC), 2013 International Conference on*IEEE.

[19] D. Hurley-Smith, J. Wetherall, and A. Adekunle, "SUPERMAN: security using pre-existing routing for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2927–2940, 2017.

[20] J. J. Garcia-Luna-Aceves, "Routing to multi-instantiated destinations: principles and applications," in *Network Protocols (ICNP), 2014 IEEE 22nd International Conference on*IEEE.

[21] R. P. Premanand and A. Rajaram, "Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2089–2098, 2020.

[22] A. Rajaram and S. Palaniswami, "Malicious node detection system for mobile ad hoc networks," *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 1, no. 2, pp. 77–85, 2010.

[23] S. Palaniswami and A. Rajaram, "An enhanced distributed certificate authority scheme for authentication in mobile ad hoc networks," *The International Arab Journal of Information Technology (IAJIT)*, vol. 9, no. 3, pp. 291–298, 2012.

[24] V. Sangeetha, M. Vaneeta, S. S. Kumar, P. K. Pareek, and S. Dixit, "Efficient intrusion detection of malicious node using Bayesian hybrid detection in MANET," in *IOP Conference Series: Materials Science and Engineering*, vol. 1022no. 1, IOP publishing, p. 012077, 2021.

[25] A. Christopher Paul, D. Bhanu, R. Dhanapal, and D. Jebakumar Immanuel, "An efficient authentication using monitoring scheme for node misbehaviour detection in MANET," in *International Conference on Computing, Communication, Electrical and Biomedical Systems*, pp. 627–633, Springer, Cham, 2022.

[26] M. Rath, B. Pati, C. R. Panigrahi, and J. L. Sarkar, "QTM: a QoS task monitoring system for mobile ad hoc networks," in *Recent Findings in Intelligent Computing Techniques*, pp. 543–550, Springer, Singapore, 2019.

[27] S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," *Sustainable Cities and Society*, vol. 79, p. 103483, 2022.

[28] X. Chen, T. Wu, G. Sun, and H. Yu, "Software-defined MANET swarm for mobile monitoring in hydropower plants," *IEEE Access*, vol. 7, pp. 152243–152257, 2019.