Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6776378, 9 pages
https://doi.org/10.1155/2022/6776378

Research Article

Novel Link Establishment Communication Scheme against Selfish Attack Using Node Reward with Trust Level Evaluation Algorithm in MANET

S. Hemalatha,[1] Pravin R. Kshirsagar,[2] Hariprasath Manoharan,[3] N. Vasantha Gowri,[4] A. Vani,[5] Sana Qaiyum,[6] P. Vijayakumar,[7] Vineet Tirth,[8] Sulaima Lebbe Abdul Haleem,[9] Prasun Chakrabarti,[10] and Dawit Mamiru Teressa[11]

[1]*Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India*
[2]*Department of Artificial Intelligence, G.H. Raisoni College of Engineering, Nagpur, India*
[3]*Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Poonamallee, Chennai, Tamil Nadu, India*
[4]*Department of Electrical and Electronics Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad, India*
[5]*Department Of Electronics and Comminication Engineering Chaitanya Bharathi Institute of Technology, Hyderabad, India*
[6]*Center of Research in Data Sciences, University Teknologi Petronas, Seri Iskandar, 32610 Perak, Malaysia*
[7]*School of Electronics Engineering, Vellore Institute of Technology, Chennai, India*
[8]*Department of Mechanical Engineering, College of Engineering, King Khalid University, Abha, 61411 Asir, Saudi Arabia*
[9]*Faculty of Technology, South Eastern University of Sri Lanka, Sri Lanka*
[10]*Techno India NJR Institute of Technology, Udaipur, 313003 Rajasthan, India*
[11]*Department of Chemical Engineering, College of Biological and Chemical Engineering, Addis Ababa Science and Technology University, Addis Ababa, Ethiopia*

Correspondence should be addressed to Pravin R. Kshirsagar; pravinrkshirsagarphd1@gmail.com and Dawit Mamiru Teressa; dawit.mamiru@aastustudent.edu.et

Received 26 January 2022; Revised 18 February 2022; Accepted 19 February 2022; Published 6 May 2022

Academic Editor: Mohammad Farukh Hashmi

Mobile network nodes are trustworthy nodes; the data access in transmitting and receiving the data packet is not efficient in different network procedures. The malicious nodes are available in routing path making the packet loss, in packet transmission for time instance. Since the regular mobile network must not verify every mobile node approved else illegal, subsequently the reserved level of nodes also was not considered, to injure the packet transmission procedure by link failure called connection loss. It minimizes the transmission rate and network lifetime and improves packet latency and energy usage. The proposed novel link establishment communication (NLEC) technique is used to find the dependable routing path against intruder node available in the network. This scheme selects genuine node for routing path production, by using the node reward with dependence level estimating algorithm to compute every node trust level and resource range, to disconnect higher trust level node and lower trust level node; higher trust level node is a genuine node which performs secure communication. Lower trust level node is selfish node and they are detected and ignored from path. It increases the lifespan of network and throughput and minimizes the end to end delay and energy consumption.

1. Introduction

Mobile network is an identity organizing wireless networks for mobile node that is self-possessed by a set of mobile incurable with wireless transceiver while the packet transmission ability injured among the common links of subordinate nodes. Divergence in the misfortune of natural failure such as noncenter dispersed controlled network can offer the temporary packet transmission distinguished with remaining information sharing in the network structure, and ad hoc network has the subsequent features [1]. The mobile network is a self-regulating topology that is active, the transmission rate is limited, and the ability of network is variable. The mobile network is movable one, where every nodes are approved to travel in dissimilar extent that outputs in dynamic network scheme; because nodes are travelling consequently, they can go out of coverage limit in the network else move towards in coverage limit of network at any instance, and any node that are part of network with routing time can be part of an remaining network at time instance [2]; mobile network is also used for meeting or one-time convention in that users preserve fast to share information and data attainment operation in warm environment.

The terminal energy is restricted and the networks are guarded among them. The communication scheme in ad hoc network is significant in obtaining better characteristics of network environment [3]. The difficulty of scheming network methods for mobile network comes from link awaiting they split that is caused by network presentation humiliation; the path redesigning of connection taking the main dispute of communication technique process is proceeded to rebuild the packets that are dropped to make quality of service of links based on the condition of network structure [4]. A quantity of mobile network routing scheme becomes proficient and accurate. There are many kinds of communication schemes in mobile network float routing against unstable else ranking routing that benefits of upbeat system for communication [5]. The routing scheme has three parts. The first one is MAC layer selection depending on arriving signal force from physical layer by means of cross layer procedure. Subsequent method is used to evaluate the link expired time instance [6]. In this scheme, the time taken for two mobile nodes to link with each other using global positioning system below different velocity in this period called routing was evaluated, ultimately to construct a latest routing path preservation method to minimize the connection failure using local path revival procedure considering every issues together, to define a parameter that effort to keep a steadiness among the velocity and energy constraint in mobile network [7]. Ad hoc networks have seen greater network latency due to an increase in collision, concealed endpoints, noise, bidirectional links, and frequent path breakdowns caused by node mobility, because the network's dynamic characteristics and changes in topology are caused by node migration.

Presently, the many path routing schemes are used to redirect all the overload among the solitary better possible path finding that often outputs in below use of network energy level. Possibly, many path communication methods can optimally divide the load depending on the precedence transversely the obtainable group of routes. Choosing the quality of service parameter for path chosen in detailed function is necessary in making a decision for the network presentation [8]. In the direction of obtaining efficient survey for discovery, multipath routing method obtaining the QoS for wire-based network structure that divides the various overloads along the rest of routes has not been explore. In the model path conditions, the network transmission speed is directly relative to the packet success rate, while in mobile network, the paths are error-level and differ in excess of time instance [9]. Therefore, the pre resolute maximum rate of data transmission and latency responsive overload output in an improved packet loss rate in excess of the path allocation corrupts the network transmission rate. The physical layer of MAC helps different broadcast mode depending on wireless path features. The data transmission rate alteration is a method to energetically alter the data forwarding rate, consequently altering the path code and inflection method [10].

Residual of the paper is designed as follows. Part II provides related works. In part III, the details of the proposed novel link establishment communication (NLEC) technique linked to establishment communication were presented, to discover the trusted routing path over link failure node present in the network. The node reward with trust level evaluation algorithm is designed to maximum trust level nodes for communication process. Part IV provides simulation performance result analysis obtained under various metrics. At last, part V concludes the paper with future process.

2. Related Works

M. A. Gawas and M. M. Gawas [11] propose a blockage attentive QoS measurements based on disjoint multipath routing scheme to course the need movement through the most productive method. Utilizing the mapping capacity among MAC and system layer, activity is part in to set of productive ways in light of need. To expand our cross-layer scheme by misusing the multirate interface adjustment capacity to choose the proper transmission rate on a casing premise, in view of the channel state data, the execution of the proposed plot is completely assessed among the recreations, which feature the upsides of our cross-layer instrument.

Kumar and Kamalakkannan [12] proposed another cross-layer conspire-based calculation to lessen the connection break in mobile network structure. This proposed three plans to diminish packet retransmission proportion by dispersion flag data between objective and MAC and to talk about the regular course disappointments in mobile network by distinguishing quickly the broken connections rather than forecast of obtained flag control. To discover enhanced course upkeep by thinking about bandwidth, packet latency results by altering of quality of service. The execution of cross-layer process for every one of the plan recreations is completed to assess the organized execution utilizing system test network simulator in view of the basic metrics like

transmission rate and packet conveyance ratio in terms of number of nodes in different interval time instance.

M. A. Gawas and M. M. Gawas [11] present MOCLO multitarget cross-layer optimization between PHY-MAC-Network layer in the wake of directing a careful investigation of 802.11e conduct over MANETs. In the first place, it actualizes every one of the lines in 802.11e as a need line scheduler to organize the transmission of the movement stream. Next, it proposes a clog mindful quality of service measurements based on disjoint multipath routing scheme to course the need activity through the most effective way. Utilizing the mapping capacity among MAC and system layer, the movement is part in to set of productive ways in light of need. It broadens our cross-layer approach by abusing the multirate connect adjustment capacity to choose the fitting transmission rate on an edge premise, in light of the channel state data. The execution of the proposed plot is altogether assessed through the reenactments, which feature the benefits of our cross-layer system.

Bakhar [13] presents cross-layer based on oddity intrusion detection system which is used to perceive vindictive hubs (intruders). IDS is used with customary AODV power and delay enhanced for discovering reasonable load adjusting way while choosing hubs. The recreated results like throughput, control utilization, and packet drop extent are differentiated among ad hoc routing, power-based ad hoc routing, and IDS regarding hub portability and reproduction time. The results exhibit that the proposed IDS outperforms for upgrading network process.

Dana et al. [14] proposed intermittent Hello packet informing a generally utilized plan to get nearby link accessibility information. This may be pointless because Hello informing can deplete batteries while cell phones are not being used. This paper proposes a versatile Hello informing plan to smother superfluous Hello messages without decreased perceptibility of broken connections. Reenactment output indicates that the proposed conspire lessens vitality utilization and system overhead with no indisputable contrast in transmission rate adopting an elective strategy, i.e., a cross-layer outline, and presenting another grouping based on directing convention named cross-CBRP. In this new approach, the connections between physical, MAC, and directing layers are completely abused to all the more likely adjust the bunching calculation to differing connection and system condition because of versatility. All the more definitely, in the proposed cross-CBRP calculation, flag control data at the physical layer is used for the directing layer with the end goal that it can amplify the strength of the framed groups. Through recreation think about utilizing the NS-2, it assesses the execution of the exhibited cross-CBRP and shows its significant execution gains.

Patil and Kerji [15] propose a framework which rejects the fault data signs obtained at the physical layer by contrasting the flag with impedance clamor proportion with the flag to commotion limit esteem. Impedance and clamor motion alongside genuine flag quality parameters are estimated at physical layer of OSI reference design. The proportion of these two parameters is computed and is cross-layered to the directing layer as a cross-layer parameter. In directing layer, it keeps up a flag to impedance clamor proportion edge esteem. SINR is contrasted to select or dispose of the related obtained message. In the event that the obtained message has SINR which is not as much as the edge esteem, such messages are disposed of. In the event that message has higher SINR when contrasted and SINRT, at that point, it is chosen for additional handling. It actualized this by rolling out improvements to AODV convention utilizing NS2 test network. The subsequent framework makes interfaces in CLAODV dependable and in this manner expands the throughput and packet conveyance proportion and decreases the postponement and overhead.

According to Amel and Zoulikha [16], with an end goal to enhance the execution of portable specially appointed system, cross-layer strategy is actualized. It intended to determine QOS issues in MANET and allows to share data about system status between various layers. It proposed a cross-layer outline among physical and steering layers utilizing obtained flag quality as cross-layer collaboration parameter. It actualizes new steering convention in light of RSS. The convention is tried with NS2 test system in free space and shadowing model and ensures an upgraded availability and dependable course development in the mobile network.

Gawas et al. [17] indicate to accomplish multilayer usefulness from physical layer to the steering layer to give agreeable correspondence. A versatile cross-layered agreeable steering calculation (ACCR) is proposed to break down the channel state varieties and specifically pick the helpful MAC plot on request by misusing spatial assorted variety. The calculation progressively chooses best hand-off competitors in view of QoS metric, dispute postponement, and hub vitality reasonableness. The network layer, at that point, picks an advanced way from source to goal through the chose transfer hubs. It approves the calculation with broad recreations. The outcomes plainly demonstrate that helpful cross-layer configuration approach adequately enhances the normal throughput and normal deferral for every packet transmission.

Gadekar and Kadam [18] proposed a novel efficient enemy of antiblocking method in view of cross-layered neighbor reliance exhibited in this paper. The channel state information (CSI) alludes to channel properties of a connection and depicts how a flag engenders from the transmitter to the collector and speaks to the joined impact of disseminating, blurring, and control rot with separation. As indicated by the neighbor reliance assessed by CSI, it is used to choose a neighboring hub as the following bounce hub will incredibly debase the transmission dependability. At last, the reenactment results demonstrate that the solid steering convention in light of neighbor reliance convention it proposed essentially beat preferred transmission dependability over the traditional calculation and the enhanced ad hoc routing in view of path connection cost evaluation.

Rath [19] proposed a scheme introducing dependable system layer convention with upgraded postponement and power for mobile ad hoc network in view of the concept of ad hoc on request distance vector routing. In spite of the fact that numerous kinds of conventions have been produced for MANET routing, yet our approach is distinctive in a way

that it computes the edge in an incentive way as an element of power consumption, bounded delay, and packet processing rate of the hub to be chosen for bundle sending towards goal in a heap adjusted manner rather than the most limited way, and besides, a cross-layer component has been presented with handshaking between information connection layer and system layer to lessen the overhead of system layer amid course finding by diminishing force utilization. The proposed convention enhances throughput in information transmission with ensured bundle conveyance and least data transfer capacity. The execution of the proposed convention is assessed utilizing NS2 network, and relative examination of this convention has been finished with other driving system layer conventions.

3. Overview of Proposed Scheme

Mobile network nodes are trustworthy nodes, and the communication like packet transmitting and receiving is not easy one for various network structures. The misbehaving nodes are present in the communication route, and it makes the packet loss and packet transmission time instance. Since the general mobile network, when processing time does not verify, whether each mobile node is protected otherwise unprotected, then resource level of nodes is also not monitored clearly; to injure the packet transmission by misbehaving node is known as selfish attack. It minimizes the transmission rate and lifespan of network and maximizes end to end delay and energy usage.

Figure 1 shows the novel link establishment communication (NLEC) technique. The sender searches the routing path in network environment, and the novel link establishment communication scheme is constructed to provide trustworthy routing. Node reward with trust level evaluation algorithm is designed to analyze the trust level of every node, and higher trust rate node is selected to perform routing; else, lower trust level node is rejected. This reduces energy usage and end to end delay.

The presented novel link establishment communication (NLEC) method is constructed, to find the protected routing path against selfish attacker node available in the network structure. This scheme is used to select genuine node for route designing. By using the node reward with trust level evaluation algorithm to analyze the every node trust value with resource level, to split maximum trust level node and minimum trust level node, the maximum trust level node is a genuine node that executes protected packet transmission. Minimum trust level node is selfish attacker node; they are identified and removed from routing path. It improves the lifetime of network and transmission rate and reduces the end to end delay and energy usage.

3.1. Source Node Pointing the Routing Path. Discovering the minimum distance route and exploring every potential routes from source node to target node, the route contains the most excellent signal quality that can be measured as better route for communication. Since the communication proceeds from end to end, the route has better signal quality, so packet delivery rate in this condition can significantly

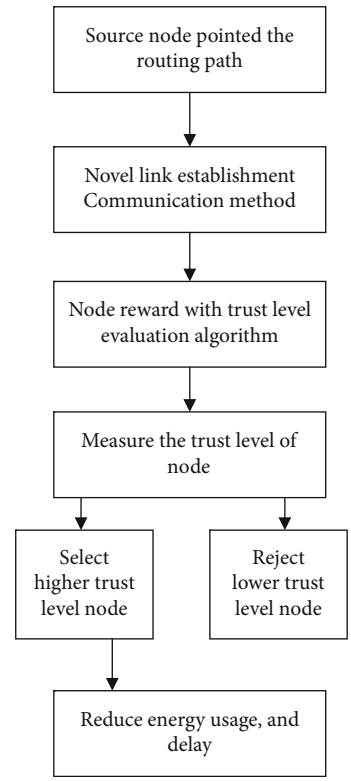


Figure 1: Block diagram of the proposed novel link establishment communication (NLEC) technique.

improve. It tends to discriminate this network as an output of process holding time instance which is maximum, though it is possible to a various path having minimum waiting time instance to an existing path. TR is trust routing, Spt is source node pointed, L is link, NL is novel link, and RT is reward with trust.

$$\mathrm{TR} = \mathrm{Spt} * L, \tag{1}$$

$$L = \mathrm{NL} + \mathrm{RT}. \tag{2}$$

The energy level of node is measured, every time once packets received by receiver node. To fix the threshold value to check whether every node resource level performs communication process at the time instance, node packet received energy level avoids threshold energy, and the node will fail. The threshold energy level is that the minimum amount of resources taken. The necessary energy level of the packet received node is estimated. Depending on the node energy level or resource availability rate to construct the routing path from source node to the destination node, the intermediate nodes are used to relay the data packet sequentially. In the recent sequent route, communication technique for end to end connection is vital. The intruder node is present in the path, and it needs to transmit an error packet to neighbor node and provide the packet transmission trying to find recent path, and sometimes attacks occurred to delay the communication for allocated time slot $(Ne + Tr)$.

The following is the node energy level with transmission rate.

$$\text{Spt} = \text{Ne} + \text{Tr}, \tag{3}$$

$$\text{TR} = (\text{Ne} + \text{Tr}) * \text{L}. \tag{4}$$

Generally, the existing rate selection schemes adopt probe depending on methods that search for the majority of best transmission rate using the knock and assessment schemes and focal point only on the active path state details, ignoring the blocking depending on factors disturbing the network transmission rate. Such a probe-based method is a consequence of suboptimal characteristics since the unproductive investigation continuously alters suitable contention metric considering the continuous alteration of the path situation. A network is thought to be jam-packed when the accessible overload exceeds the present resource availability. Such a situation leads to improved buffer space required in relay nodes in excess of the data route, which in turn improves the packet loss rate considering the restricted resource presence. This output in retransmission time exceeds data packets, which additionally degrades the network transmission rate.

3.2. Novel Link Establishment Communication (NLEC) Technique. Monitor the node's location and packet transmission continuously; this surveillance part is determined on aggregation and measuring of process performed in specific location; the characteristics of the nodes add to the trust estimation. Consider that these data packet can be forwarded depending on connections among intermediate nodes; the clarification of communication processes as well as estimation and suggestion was disseminated within the network environment. For the time instance, the accuracy of the packet relaying can be checked from end to end measurement of receiving reply or monitoring the packets transmitted by the observing node. $M(\ln) * p$ is monitor node location with path establishment. $R(\text{traffic})$ is removing traffic.

$$\text{NL} = M(\ln) * p, \tag{5}$$

$$p = R(\text{traffic}). \tag{6}$$

For an efficient differentiation service schedule for various access queue by constructing a link establishment between the nodes, the MAC and the network layer backlog for each of the access nodes, depending on its quality of service requirement. Packet drop causing latency sensitive uses consider to blocking or path disappearing setting is a main problem in mobile network. Presently, in most of the previous multipath communication techniques, all the overload is routed through a solitary route. In routing the maximum precedence overload alongside with the low precedence overload output in extra latency for high precedence overload, it is also important to consider the misuse of network possessions. Therefore, to enhance the presentation of real-time uses and improve the path usage, the broadcast of a quantity of packets must accept the dissimilar fault and loss safety for which it obtains various routes for each category of service. Whether the source node and target node are similar for the maximum and minimum loads, the algorithm links the main efficient route established to broadcast the maximum precedence packets, although the lower precedence packets get forwarded among the alternative many effective routes. This path provides quality of service level to the uses involving similar route for best attempt data forwarding.

$$\text{NL} = M(\ln) * R(\text{traffic}), \tag{7}$$

$$\text{NL} = M(\ln) * R(\text{overload}). \tag{8}$$

The identification of selfish node in communication process such irregular with protection condition undertaken by processing node should proceed among the distinguishing of information on sensitivity of relaying data present in the packet header with the trust level to measure the intermediate nodes in the network structure. The data on trust level to neighboring nodes should be collective within the network environment and maintain the deduction and organization procedures. Algorithm 1 for novel link establishment communication scheme is vital, only for group of data packets transferred. The present scheme result uses a timing of routing path to obtain primary protection and customized interference chains are removed, to protect packet transmission and measure the confirmation significance. This is vital that mobile network nodes, network topology, central protection structural design, and recordability ability are essential. The protection mechanism is incorporated with the presented trust organization mechanism which does not use extra details of unit transmission technique. The present scheme allows the protection mechanism to reply on process created by the trust managing actions.

3.3. Node Reward with Trust Level Evaluation Algorithm. The trust value is estimated at every node for its direct individual neighbor node in the path. In the packet sent by the sender node, it is also retransmitted to the similar node, because of minimum protection level of nodes. By means of the ratio of the entire amount of packets send from a source node to its nearest neighbor node to the entire quantity of packets are received reverse from the similar neighbor node in the path. The selfish node hides the information that time interference occurred; they are detected and removed by using this algorithm, to verify the trust level of every node available in the routing path. Tl is trust level measurement.

$$\text{RT} = \text{Tl}, \tag{9}$$

$$L = M(\ln) * R(\text{overload}) + \text{Tl}, \tag{10}$$

$$\text{TR} = \text{Spt} * M(\ln) * R(\text{overload}) + \text{Tl}. \tag{11}$$

In Algorithm 2, node reward with trust level evaluation algorithm is constructed to measure the intermediate node trust level. This algorithm needs to separate the maximum trust level and minimum trust level node. The maximum trust value node is selected to construct the interference free

Step 1: Construct the routing path from source to destination node
Step 2: for each node discover protected routing
Step 3: source node search the routing path
Step 4: if $\{Path! = interference\}$
Step 5: trustworthy node to perform communication
Step 6: *else* if $\{Path == interference\}$
Step 7: selfish node to block communication
Step 8: End if
Step 9: End for

Algorithm 1: Algorithm for novel link establishment communication technique.

Step 1: Calculate the trust level of every node
Step 2: for each node search trust path
Step 3: if $\{trust\ level == high\}$
Step 4: These nodes are used to design path
Step 5: *else* if $\{trust\ level == low\}$
Step 6: These nodes are rejected from path.
Step 7: end if
Step 8: Enhance Throughput
Step 9: End for.

Algorithm 2: Node reward with trust level evaluation algorithm.

routing path. It improves throughput and network lifetime and minimizes energy consumption and end to end delay.

Packet ID. Packet ID contains every mobile node communication details. The node location, node connectivity, and transmission rate of nodes are maintained in specific routing table

In Figure 2, the proposed novel link establishment communication (NLEC) method packet format is shown. Here, the source and destination node ID field each takes three bytes. Third one is source node pointed the routing path that takes three bytes, to establish the link between mobile nodes. Novel link establishment communication technique offering the connection is vital, only for group of data packets transferred. The fourth field takes two bytes. Node reward with trust level evaluation algorithm is constructed to measure the intermediate node trust level. The fifth occupies three bytes and measures the trust level of node. This algorithm needs to separate the maximum trust level and minimum trust level node. The maximum trust value node is selected to construct the interference free routing path. It improves throughput and network lifetime and minimizes energy consumption and end to end delay.

4. Performance Evaluation

4.1. Simulation Model and Parameters. The proposed novel link establishment communication (NLEC) technique is simulated with Network Simulator (NS2.34) tool. In our simulation, 100 mobile nodes are placed in a 1074 meter × 1062 meter square region for 25 milliseconds simulation time. Each mobile node goes random manner among the network in different speed. 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 obtain effective connection among unstable mobile nodes. Table 1 shows the estimation of simulation setup.

Simulation Result. Figure 3 shows that the proposed novel link establishment communication (NLEC) method to link establishment communication, to discover the trusted routing path over link failure node present in the network, is compared with existing SOL [18] and TES [20]. The node reward with trust level evaluation algorithm is designed to maximum trust level nodes for communication process. It improves throughput and network lifetime and minimizes energy consumption and end to end delay

4.1.1. Performance Analysis. In simulation, the following performance metrics using X graph in NS2.34 were analyzed.

(1) End to End Delay. Figure 4 shows end to end delay estimated by the amount of time used for packet transmission from source node to destination node; node reward with trust level evaluation algorithm is constructed to measure the intermediate node trust level. In the proposed NLEC method, end to end delay is reduced compared to existing scheme ECAR, SOL, and TES.

$$\text{End to End Delay} = \text{End Time} - \text{Start Time} \quad (12)$$

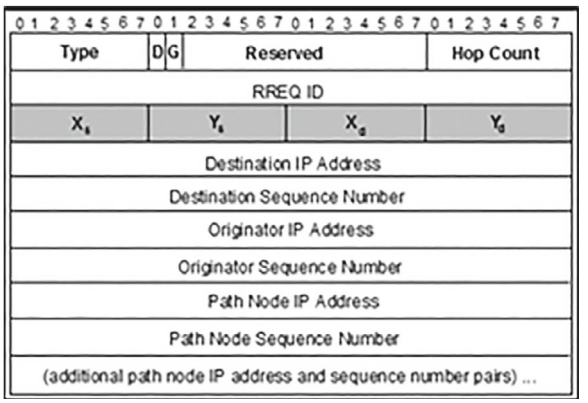
(2) Communication Overhead. Figure 5 shows communication overhead which is minimized in which sender transmits packet to receiver node and node reward with trust level evaluation algorithm. This algorithm needs to separate the maximum trust level and minimum trust level node. In the proposed NLEC method, communication overhead is reduced compared to existing scheme ECAR, SOL, and TES.

$$\text{Communication overhead} = (\text{Number of Packet Losses/Received}) * 100 \quad (13)$$

(3) Throughput. Figure 6 shows throughput measured by no. of received from no. of packet sent in

Source ID	Destination ID	Source node pointed the routing path	Novel link Establi shment comm unication	Node reward with trust level evaluation algorithm	Measure the trust level of node
3	3	3	2	2	3

(a) Proposed NLEC packet format



(b) Proposed route packet format

Figure 2

Table 1: Simulation setup.

No. of nodes	100
Area size	1074 × 1062
MAC	802.11 g
Radio range	250 m
Simulation time	25 ms
Traffic source	CBR
Packet size	512 bytes
Mobility model	Random way point
Protocol	DSDV

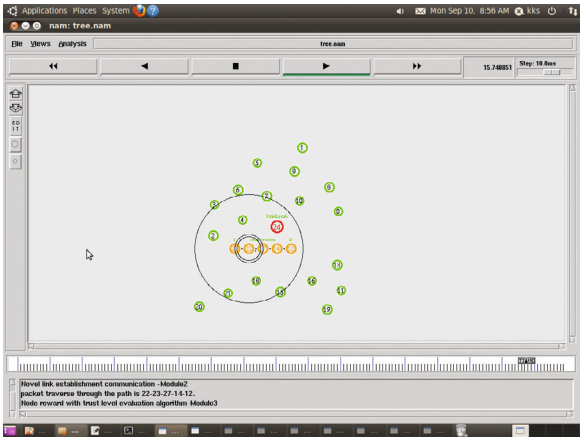


Figure 3: Proposed NLEC result.

particular speed. Node velocity is not a constant, and simulation mobility is fixed at 100 (bps). In the proposed NLEC method, packet delivery ratio is improved compared to existing scheme ECAR, SOL, and TES.

$$\text{Throughput} = (\text{Number of packet received/Sent}) * \text{speed} \quad (14)$$

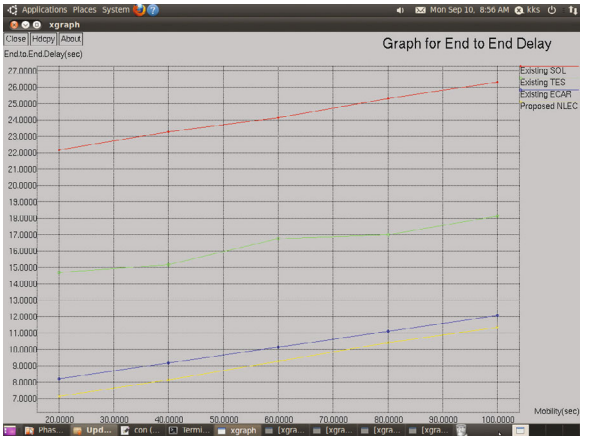


Figure 4: Graph for mobility vs. end to end delay.

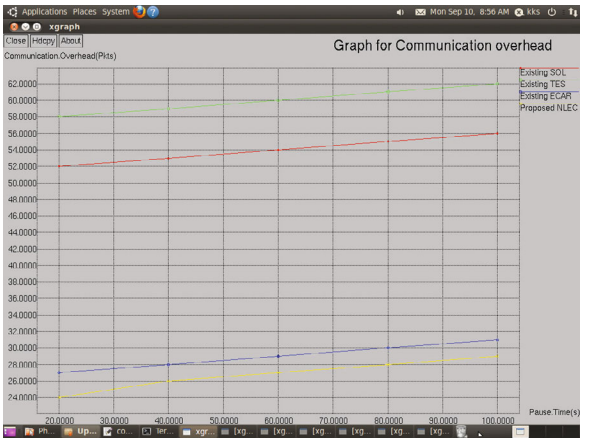


Figure 5: Graph for pause time vs. communication overhead.

(4) Detection Efficiency. Figure 7 shows detection efficiency; attacks occurred and packet transmission is repeated from source node to destination node. Novel link establishment communication (NLEC) method obtains the efficient connection between

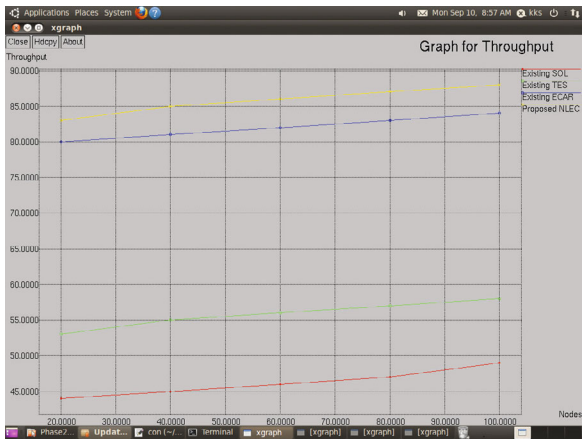


Figure 6: Graph for nodes vs. throughput.

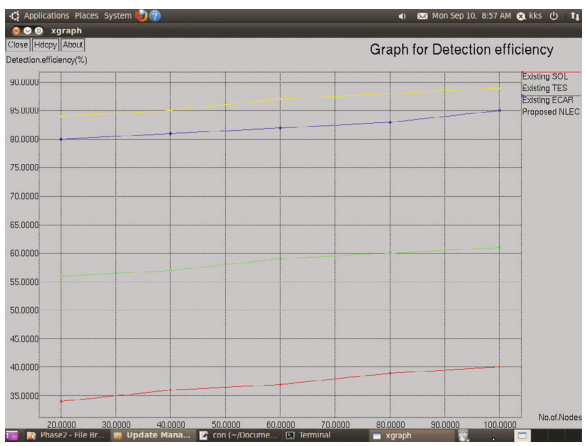


Figure 7: Graph for nodes vs. detection efficiency.

nodes. In the proposed NLEC method, the detection efficiency is improved compared to existing scheme ECAR, SOL, and TES.

$$\text{Detection efficiency} = \text{attack detection rate/overall time} \tag{15}$$

(5) Network Lifetime. Figure 8 shows that lifetime of the network is measured by node process, the time taken to utilize network from the overall network ability. In the node reward with trust level evaluation algorithm, the maximum trust value node is selected to construct the interference free routing path. In the proposed NLEC method, network lifetime is increased compared to existing scheme ECAR, SOL, and TES.

$$\text{Network Lifetime} = \text{time taken to utilize network/overall ability} \tag{16}$$

(6) Packet Drop Rate. Figure 9 shows that packet loss of particular communication in network is calculated

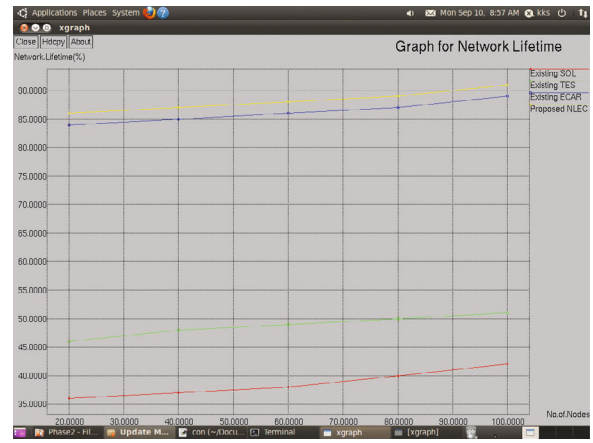


Figure 8: Graph for nodes vs. network lifetime.

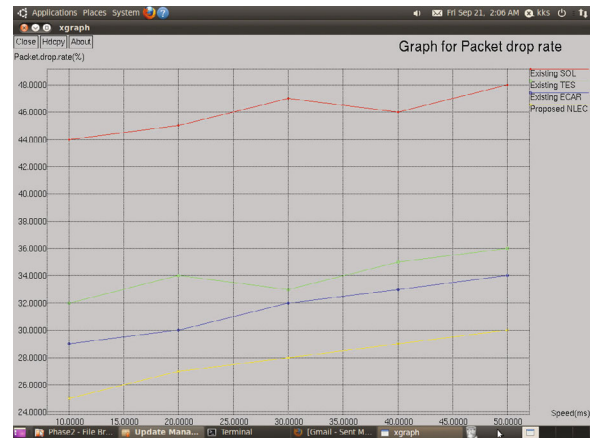


Figure 9: Graph for speed vs. packet drop rate.

by node loss packet with inefficient connection removed by using novel link establishment communication (NLEC) method. In the proposed NLEC method, the packet drop rate is reduced compared to existing scheme ECAR, SOL, and TES.

$$\text{Packet drop rate} = \left(\text{Number of packet}\frac{\text{dropped}}{\text{Sent}}\right) * 100 \tag{17}$$

5. Conclusion

Mobile network nodes are reliable nodes; the data access for communication is difficult. The misbehaving nodes are loss the data packet in communication time instance. Since the normal mobile network must not verify the nodes' authority, to break the communication process is known as selfish node. It reduces the throughput and network lifetime and increases end to end delay and energy consumption. Then, the novel link establishment communication (NLEC) technique is proposed, to find the protected communication route against the selfish attacker node. This scheme selects genuine node for routing path designing, by using the node

reward with trust level evaluation algorithm to analyze every node protection level and resource range, to split the higher trust level and lower trust level node. Higher trust level nodes are used for routing process. It increases the lifetime of network and throughput and minimizes the end to end delay and energy consumption. In future work, use cross-layer-based uncertainty communication to analyze different 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

The authors declare no conflict of interest.

Acknowledgments

The authors gratefully acknowledge the Deanship of Scientific Research, King Khalid University (KKU), Abha-Asir, Kingdom of Saudi Arabia, for funding this research work under the grant number RGP.2/89/41.

References

[1] Ahmed Loutfi and Mohammed Elkoutbi, "Energyaware clustering algorithm for the OLSR protocol," *IJCSNS International Journal of Computer Science and Network Security*, vol. 15, no. 7, pp. 85–91, 2015.

[2] P. K. Saini, Y. M. Sharma, and S. Mukherjee, "Analysis AODV, DSR&DSDV protocols with uniform pause & speed type over CBR&TCP connections in VANET," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 1512–1520, 2013.

[3] K. Bhagchandani and Y. M. Sharma, "Exploration of VANET mobility models with new cluster based routing protocol," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 6, pp. 224–227, 2013.

[4] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, New Orleans, LA, USA, 1999.

[5] A. Al-Maashri and M. Ould-Khaoua, "Performance analysis of MANET routing protocols in the presence of self-similar traffic," in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, pp. 801–807, Tampa, FL, USA, 2006.

[6] S. K. Dhurandher, S. Misra, M. S. Obaidat, V. Bansal, P. Singh, and V. Punia, "An energy-efficient on-demand routing algorithm for mobile ad-hoc networks," in *2008 15th IEEE International Conference on Electronics, Circuits and Systems*, pp. 961–995, Saint Julian's, Malta, Aug. 31 2008.

[7] H. Y. Zhang, M. E. Bialkowski, and J. Hamer, "An extended AODV protocol for VoIP application in mobile ad hoc network," *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 7, no. 2, pp. 836–841, 2009.

[8] R. Ghanbarzadeh and M. R. Meybodi, "Reducing message overhead of AODV routing protocol in urban area by using link availability prediction," in *2010 Second International Conference on Computer Research and Development*, pp. 274–279, Kuala Lumpur, Malaysia, 2010.

[9] A. Tripathi and R. Kumar, "MECB-AODV: A modified energy constrained based protocol for mobile ad hoc networks," *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 3, no. 6, pp. 15–30, 2012.

[10] X. Li, T. Liu, Y. Liu, and Y. Tang, "Optimized multicast routing algorithm based on tree structure in MANETs," *China Communications*, vol. 11, no. 2, pp. 90–99, 2014.

[11] M. A. Gawas and M. M. Gawas, "Efficient multi objective cross layer approach for 802.11 e over MANETs," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 582–587, Limassol, Cyprus, 2018, June.

[12] R. S. Kumar and P. Kamalakkannan, "A review and design study of cross layer scheme based algorithm to reduce the link break in MANETs," in *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*, pp. 139–143, Salem, India, 2013, February.

[13] P. M. D. Bakhar, "MAC layer intrusion detection system by cooperation of cross layer in MANET," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 1-2 Aug. 2017.

[14] A. Dana, A. Yadegari, M. Hajhosseini, and T. Mirfakhraie, "A robust cross-layer design of clustering-based routing protocol for MANET," in *2008 10th International Conference on Advanced Communication Technology*, vol. 2, pp. 1055–1059, Gangwon, Korea (South), 2008, February.

[15] R. Patil and V. K. Kerji, "SINR based routing for mobile ad-hoc networks," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 5, pp. 369–372, Kanyakumari, India, 2011, April.

[16] B. Amel and M. M. Zoulikha, "Routing technique with cross-layer approach in ad hoc network," in *2009 Second International Conference on the Applications of Digital Information and Web Technologies*, pp. 313–318, London, UK, 2009, August.

[17] M. A. Gawas, L. J. Gudino, and K. R. Anupama, "Cross layered adaptive cooperative routing mode in mobile ad hoc networks," in *2016 22nd Asia-Pacific Conference on Communications (APCC)*, pp. 462–469, Yogyakarta, Indonesia, 2016, August.

[18] S. Gadekar and S. Kadam, "Secure optimized link state routing (OLSR) protocol against node isolation attack," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pp. 684–687, Chennai, India, 2017, September.

[19] M. Rath, "Optimized network layer protocol with cross layer handshaking mechanism in MANET," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1–10, Coimbatore, India, 2016, January.

[20] P. K. Sharma, U. Tiwari, and Y. M. Sharma, "A throughput efficient on-demand steering procedure for mobile ad hoc networks," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 1010–1015, Palladam, India, 2017, December.