ISSN NO: 9726-001X
Volume 08 Issue3 July2020

JOURNAL OF CURRENT SCIENCE

A SAFE AND EFFECTIVE APPROACH TO EXTENDING THE LIFE OF WSNS WITH MOBILE ADHOC-BASED CPS

Q.AJAYA KUMAR
K.J.L InstituteAssistant Prof. E&C dept.
of Technology Channai

Abstract

Recent developments in wireless communication and network security have made it feasible to design networks that can reliably link and run a large number of devices. In static networks, energy savings are guaranteed by using efficient topology control strategies. The best platform for building networks is a mobile ad hoc based CPS. There are significant research hurdles for the design to overcome, such as increasing the created network's connection while decreasing energy consumption and end-to-end latency. A new method, dubbed mobility aware local tree based reliable topology (MA-LTRT), is proposed, together with a reliable route design algorithm, to solve these research issues. This project also takes the necessary precautions to ensure data security. Therefore, the Blowfish algorithm is added as a security mechanism that guarantees the information's veracity and keeps it secure throughout transmission.

Mobile Ad-hoc CPS, Energy, Network, and MA-LTRT are some of the Keywords to look for.

I.INTRODUCTION

Many scientists are drawn to the cyber physical system because it offers accurate modeling of the physical system, making it an essential co-domain in network security. In addition, mobile ad hoc networks (MANETs) provide significant prospects for study since they reduce power consumption while simultaneously enhancing network connection. Topology control techniques assure the energy savings in static networks. Rather of giving a single value to the whole network, topology control algorithms will allow each node to independently determine the transmission power it needs. As a result, this research endeavor is dedicated to measuring the impact of node relocation on network performance. Local Minimum Spanning Tree (LMST) [3] and Local Tree-based Reliable Topology (LTRT) [2], which may provide reliable topology for static networks, are considered as part of the research. Using these methods as a foundation, a new, "mobility aware," characteristic feature is provided, as well as a design and proposal for a local tree-based, trustworthy topology that takes mobility into account. In addition to reducing power consumption and improving network connection, this project's most significant contribution is the provision of data security and authentication [1]. Therefore, the utmost caution is used to transfer the data quickly and accurately. The "Blowfish algorithm" is employed to encrypt the data.

OVERVIEW OF THE EXISTING TOPOLOGIESCONTROL METHODS AND THEIR SHORTCOMINGS

Numerous techniques for topology control have been presented in the past. These techniques include things like Local minimum spanning tree (LMST), Local tree based reliable topology (LTRT), and Cone based distributed topology control (CBTC). Li et al. [4] created the CBTC topology.

In CBTC, each node determines its own transmission range so it may communicate with its nearest neighbors, who are located on the fan-shaped network topology. They make contact at an angle defined by. Since the likelihood of an adjacent node's existence increases as increases, all nodes may reduce their transmission range when is greater.

This is supported by the observation that network connection is guaranteed for the value of [4] when 5=6. One of the problems with the CBTC is that it results in excessively redundant network topologies. Therefore, more energy is needed to support this topology. The LMST is a topology control approach that takes into account the characteristics and layout of a tree's structure [5, 6]. In LMST, each node uses information from just its nearest neighbors to build a topology based on the MST (Minimum Spanning Tree) [7]. Since LMST generates a directed graph for the topology, auxiliary messages are required for the non-directed graph to be computed.

.

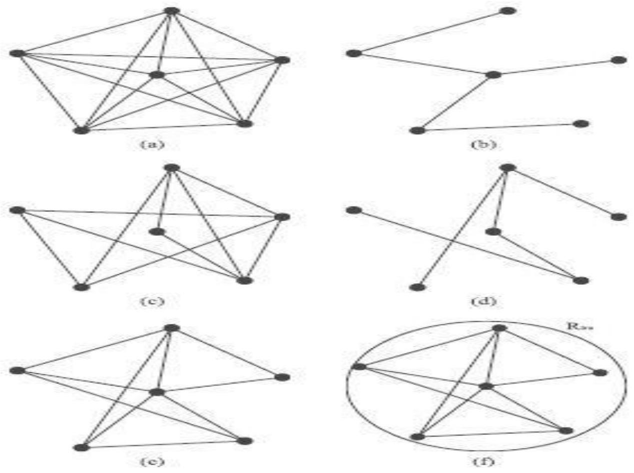


Fig 2.1 An example of construction of topology in LTRT
(a) Complete tree, (b) 1st MST, (c) (a)-(b), (d) 2ns MST
(e) (b)+(d), (f) Setup of radius

In LMST, each node uses information from just its nearest neighbors to build a topology based on the MST (Minimum Spanning Tree) [7]. This LMST-generated topology, however, is a directed graph, therefore calculating the non-directed graph requires additional messages. Based on LMST and Tree-based Reliable Topology (TRT) [8, 9], LTRT [8] generates topologies.

This method guarantees k-edge connectivity, meaning that the network will remain operational even if some connections fail. An example of a node constructing a topology with LTRT redundancy set to two is shown in Fig. 2.1.The whole tree formed by these six nodes is shown in Fig. 2.1(a).

As can be shown in Fig. 2.1(b), when a node uses a tree to store topological data, it prefers a first MST. The node now selects a different MST from the tree, eliminating the initial MST from the whole tree in the process. As seen in Fig. 2.1(c), this is the case.

As can be seen in Fig. 2.1(d), the second MST eventually becomes completely independent of the first. The primary reason for using LTRT for this kind of CPS is the efficiency with which it manages "redundancy" (i.e., redundant network connection).

II. A RELIABLE, LOCAL TREE-BASED TOPOLOGY THAT TAKES MOBILITY INTO ACCOUNT

The original LTRT algorithm simply considered the two parameters of communication range and node energy. The factor of distance was ignored. As a result, this project takes into account and plans for the distance parameter. This project regulates four primary factors: energy use, average node speed, network connection, and delay.

When comparing the number of successfully received message packets to the total number of packets sent, we get the Packet delivery ratio (PDR). The PDR may be enhanced by jointly analyzing energy, distance, and communication range. In this case, packet transport is taken into account.

In the event of a node failure during transmission, the protocol calls for the message to be routed through the node that offers the shortest path. The most significant development in this project is the increased security of transmitted data, which is essential for establishing the veracity of communications and protecting them from snooping third parties.

METHEDOLOGY

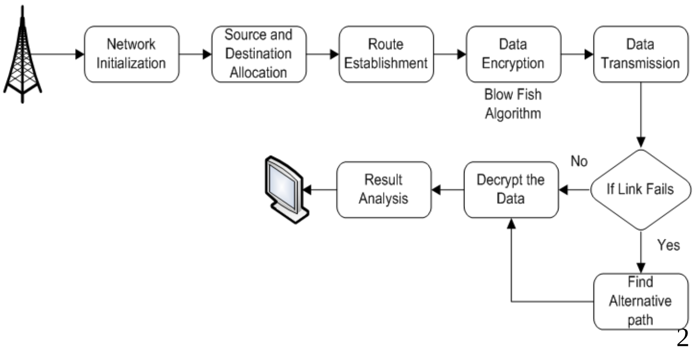


Fig 2.2. Architecture of proposed MA-LTRT method

The improved version of LTRT could providereliable communication in the mobile ad-hoc networks to an extent as it preserves a certain level of redundancy of network connectivity.

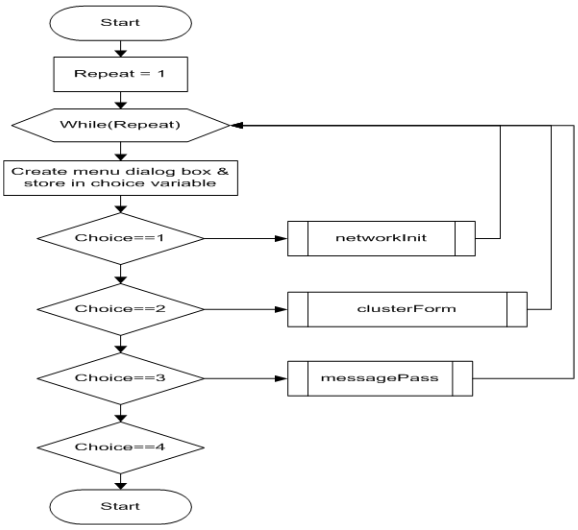
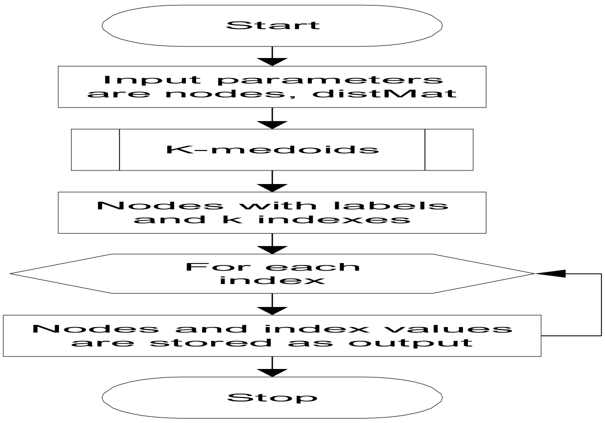


Fig 2.3. The overall Flowchart of the MA-LTRT

The Figure 2.2 depicts the Block architecture of the proposed MA-LTRT method and fig 2.4 shows flowchart. The network of the nodes present within the Mobile Ad-hoc are initialized, which further starts forming into topology depending upon the MA-LTRT topology algorithm. Further, the Cluster heads and the other branches are formed. Thecluster head broadcasts the “HELLO” Message to the neighbouring nodes, this process is termed as “Beaconing”. When the beaconed message is accepted by the free node the topology is formed with respect to the Cluster head.


Start
Input parameters are nodes, distMat
K-medoids
Nodes with labels and k indexes
For each index
Nodes and index values are stored as output
Stop

A1. NETWORK INITIALIZATION

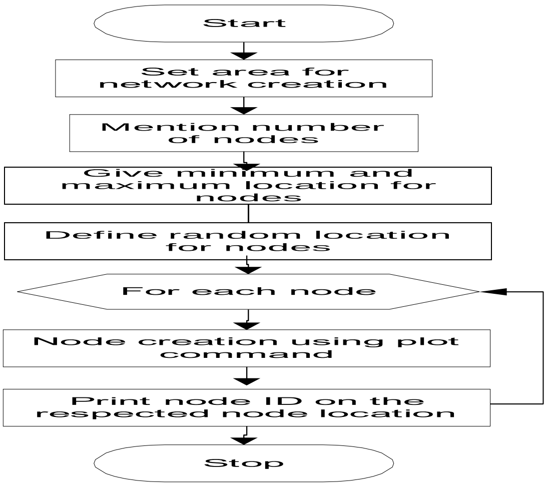

Start
Set area for network creation
Mention number of nodes
Give minimum and maximum location for nodes
Define random location for nodes
For each node
Node creation using plot command
Print node ID on the respected node location
Stop

Fig 2.4 Network initialization process flowchart

As shown in fig 2.4, for network initialization, the 100x100mm area dimension is used with number of nodes as 20, with the location of x and y, respectively. Setting initial parameter for nodes like type of nodes, node identification (node ID), node energy and setting the node size.

Fig 2.5 Reliable path establishment process flowchart

As shown in fig 2.5, the allocation of source and destination nodes is done manually during execution process.For reliable establishment of the path, the vital parameters necessary for this are source, destination and intermediate nodes. Note that all these 3 parameters act as the inputs. The transmission range is considered as 30m.

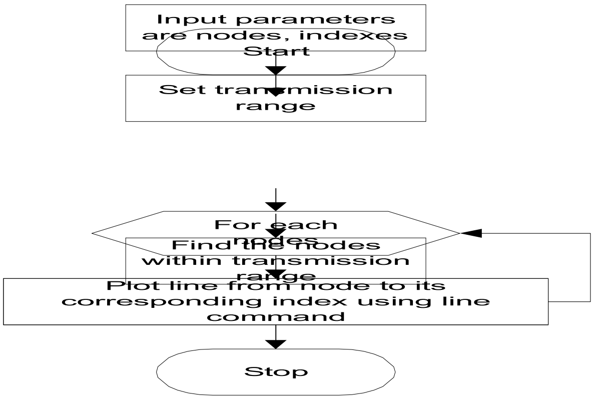

Input parameters are nodes, indexes
Start
Set transmission range
For each nodes
Find the nodes within transmission range
Plot line from node to its corresponding index using line command
Stop

Fig 2.6. Transmission range setting process flowchart

A2. CHOOSING A START POINT AND FINAL RESIDENCE

At the time of execution, the user inputs the source and destination node numbers to determine which node would be used to transfer the data.

A3. ESTABLISHMENT OF A SECURE ROUTEIf the range is within the transmission range, the data is sent immediately; otherwise, the nodes within the range must be identified, and the route with the fewest hops between them must be chosen for transmission, as seen in fig 2.6. The shortest node has been dubbed "Ranged nodes" for simplicity's sake. This procedure is continued until the message has been successfully conveyed.When calculating the shortest route, each intermediate destination serves as the source for the next node up the hierarchy, and so on, until the message is completely sent.

A4. ENCRYPTION

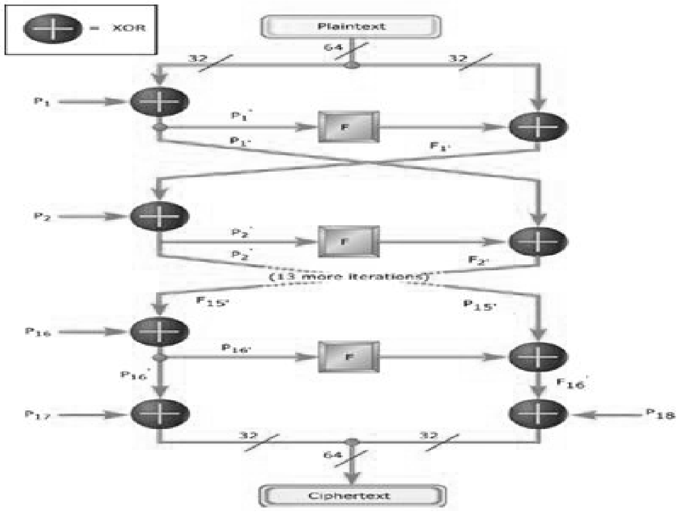


Fig 2.7. Blowfish algorithm flowchart

In this project, it was crucial to think about the whole message and break it down into user data sub-segments before transmitting it, as seen in fig 2.7. Only if this is accomplished can the message be conveyed effectively. Accordingly, the Blowfish algorithm, which has been explored, is adequate for this purpose. Furthermore, the data transmission is carried out using the preselected routers. The failure detection at each node has also been completed. In this case, the link condition is that an alternate route must be identified if the link is not equal to 0.

Data Decryption 5.

The data (beaconing message) is assumed to be 1Kb in size, whereas the message size is set at 4Kb. There will be no changes to these dimensions over the course of the project. The data send function on the receiving end performs the decryption using the blowfish technique. The recipient is then presented with the plaintext once encryption has been removed. After determining the redundant transmission range, the MST reconstruction process is repeated. Finally, given the previous architecture, we do an examination of the power utilized and the network's connection, making notes and displaying charts. Therefore, we get our information by carefully analyzing their performances and keeping track of the graphs we notice.

A. ALGORITHM OF THE MA-LTRT ALGORITHMWITH DATA SECURITY

The algorithm of the MA-LTRT method is given below with the sequential steps of execution.

(1) Initialization of Network with 20-30 numbers of nodes randomly allocated location with area of 100X100.Selection of Source and Destination nodes.

(2) Establishment of Route from source and destination using shortest path algorithm by measuring minimumEuclidean distance.

$$Euclidean\ Distance = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

(3) Encryption of Data using Blow Fish Algorithm and Transmit the data.

(4) Check whether all the nodes are active or not. If
Link failures, find the alternative path. The Data Decryption and receive the data and performance analysis is performed

II THE RELIABLE ROUTE ESTABLISHMENTALGORITHM

In AODV, the first RREQ (Route request) to arrive at the destination is used to decide the path along which data is sent from the source node[10].
The RRS algorithm proposes a stable zone and a warning zone determined by the location, velocity, and heading of a mobile node gleaned from a global positioning system (GPS).
Zones of Safety and Precaution A.

The term "stable zone" is used to describe a region where a mobile node may reliably communicate with its neighboring node.

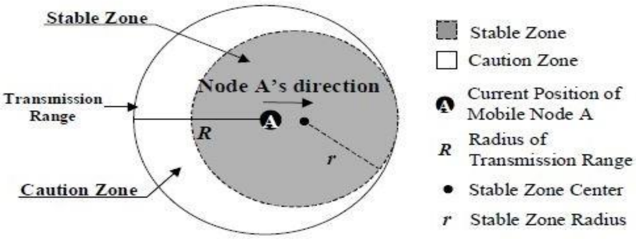


Fig 2.8 Stable Zone and Caution Zone

Caution zone, as seen in fig. 2.8, is the region in which a moving node may maintain a weak connection to its neighbors. These regions are used to determine whether a given connection state between two nodes is trustworthy.The mobile node's speed and direction data dynamically alter the boundaries of the stable zone and the warning zone.

1. Explanation of the Protocol

Using the ideas of a "stable zone" and a "caution zone," we describe the Reliable Route Selection (RRS) algorithm, and we talk about how to implement it in the route discovery phase of the current on-demand routing protocol (i.e., AODV)[10]. In this endeavor, AODV will be rebranded as AODV-RRS. When a route discovery is to be done, the source will launch an AODV RREQ control packet, and the GPS data will be added to this packet. Following is a list of the new parameters: [current_mn_position (x, y), stable_zone_center (x', y'), stable_zone_radius (r)].

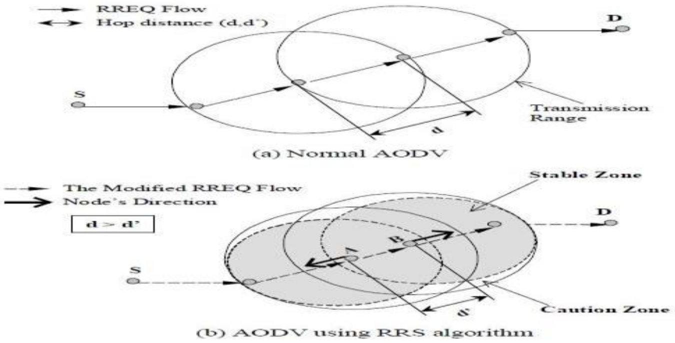


Fig 2.9 The Comparison of RREQ Flow

A mobile node's current location is indicated by current_mn_position (x, y), the center of the stable zone is shown by stable_zone_center (x', y'), and the radius of the stable zone is indicated by stable_zone_radius (r). RREQs are flooded to the destination using AODV and AODV-RRS, as seen in Fig. 2.9.

During AODV route discovery, an intermediate node will send out a flood of RREQ requests to other nodes whenever it gets a request RREQ, with the exception of when it receives a duplicated RREQ and is not physically located at the destination.

Assume that two nodes along the chosen path are situated just outside of each other's transmission range (the danger zone shown in Fig. 2.8). Due to the potential for higher hop-counts in AODV-RRS (in Fig. 2.9, note the difference in hop distance (d > d')), a route formed by AODV-RRS may incur greater transmission delay than a route established by AODV.

In this evaluation, it is considered that a mobile node may travel at most 12.5 meters per second. Therefore, finding the best solution to the equation stable_zone_radius(r) is crucial.

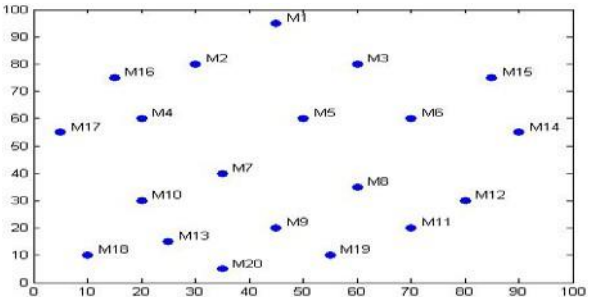
SMN (1) = R - x r

In this setting, the stable_zone_radius(r) may be calculated as stated in equation 1: where R is the transmission range of a mobile node, SMN is the speed of the mobile node, and is a constant number that sets the range of stable_zone_radius(r). The greater the value of, the more dependable the route, but the more hops there will be.

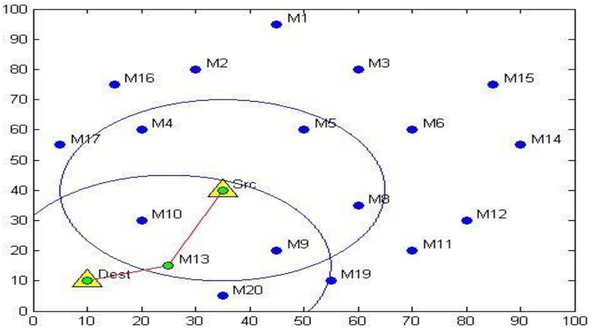
IV ANALYSIS OF RESULTS

The accompanying functional charts describe the execution order of this project. Data encryption, transmission, connection failure, retransmission, energy usage, end-to-end latency, and average node speed are all shown graphically, along with the order in which they occur in the network's operation.

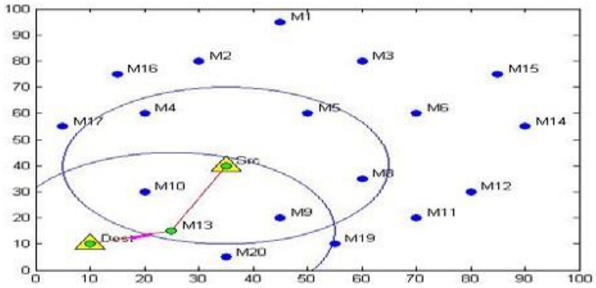
- **Network Initialization**



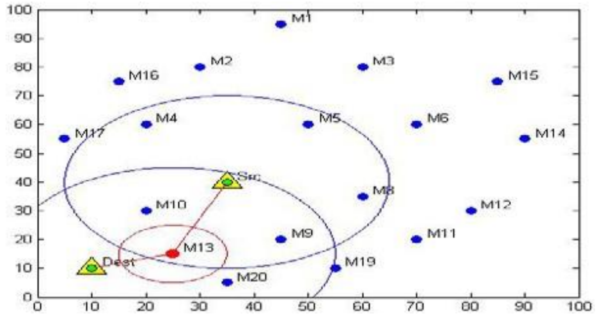
- **Source(SRC.) and Desination(DEST.) selectionwith the Route Establishment**

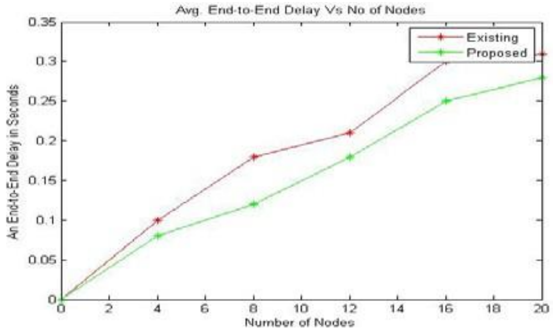


- **Data Transmission from SRC. TO DEST.**

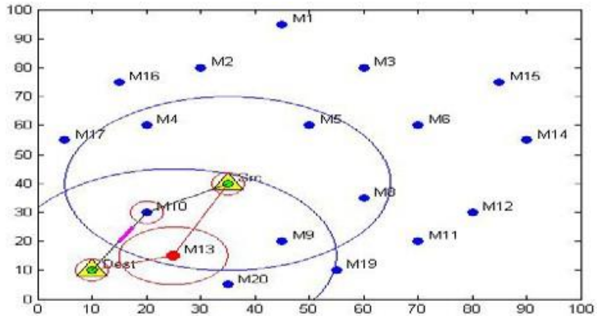


- **Fault node detection**

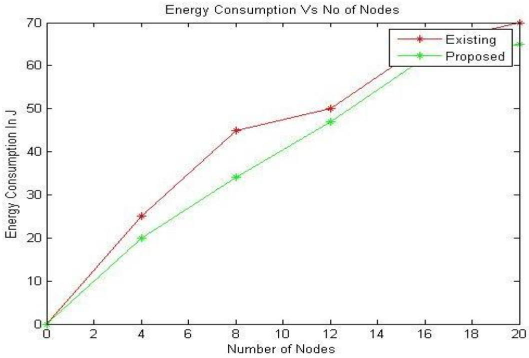




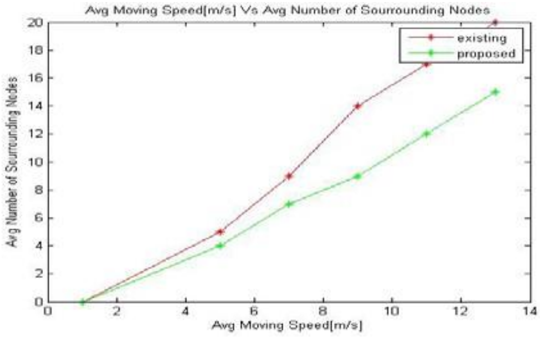
- **Re – transmission of the message by using shortestpath available**



- **Energy consumption v/s number of nodes plot to compare the existing and proposed methods energies**



- **Average end-to-end delay v/s number of nodes plot to compare the existing and proposed methods delaysAverage moving speed v/s average number of surrounding nodes plot to compare the existing and proposed methods average moving speed**



V CONCLUSION

After carrying out the recommended procedure and analyzing the obtained findings, it was determined that the design adequately addresses the design problems. As can be seen from the plots produced after execution, the design challenges of enhancing network connection while reducing energy usage and end-to-end latency between nodes have been addressed.An efficient mechanism for dynamically re-establishing the connection right after link failure is also presented in this suggested approach. It was crucial in enhancing network connections.

REFERENCES

An online optimization technique for control and communication codesign in networked cyber-physical systems, IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 439_450, February 2013. [1] C. Xianghui, C. Peng, C. Jiming, and S. Youxian.

''Radio resource management for QoS assurances in cyber-physical systems,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1752_1761, Sep. 2012, L. Shao-Yu, C. Shin-Ming, S. Sung-Yin, and C. Kwang-Cheng.

Intelligent transportation spaces: vehicles, traffic, communications, and environments,'' [3] Q. Fengzhong, W. Fei-Yue, and Y. Liuqing.

IEEE Communications Magazine, November 2010, Volume 48, Issue 11, Pages 136–142.

Using data from [4] M. Bahramgirim, M. Hajiaghayi, and V. S. Mirrokni,

Wireless multi-hop networks that use fault-tolerant, three-dimensional distributed topology control methods. 179_188 in Wireless Networks, volume 12, issue 2, March 2006.

An MST-based topology control algorithm: design and analysis, by N. Li, J. Hou, C. Sha, and L. Sha[5] Reference: IEEE Transactions on Wireless Communications, Volume 4, Issue 3, Pages 1195–1206.

Applications of k local mst for topology control and broadcasting in wireless ad hoc networks, IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 12, pages 1057_1069, Dec. 2004; X. Y. Li, Y.Wang, andW. Z. Song.

Reference: [7] N. Li, J. C. Hou, and L. Sha, "Design and study of an MST-based topology control method," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer Society, April 2003, pages 1702–1712.

An Efficient and Reliable Topology Control Algorithm for Ad-hoc Networks, LTRT, K. Miyao, H. Nakayama, N. Ansari, and N. Kato, IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. 6050_6058, December 2009.

Efficient and reliable link status information distribution, IEEE Commun. Lett., vol. 8, no. 5, pp. 317_319, May 2004; [9] N. Ansari, G. Cheng, and R. N. Krishnan.

According to [10] "Ad-hoc on-demand distance vector routing" by C.E. Perkins and E.M. Royer, published in Proceedings of the WMCSA'99, pages 90-100, February 1999.