Flat Velocity And Connection Trustworthiness Based Efficient Path Finding In Mobile Ad Hoc Network

S.PRABU M.C.A.,M.Phil
GUEST LECTURE,
PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE,
GOVERNMENT ARTS COLLEGE,
UDUMALPET.

Abstract: Mobile network velocity of node movement is not smooth, since it travels along various directions in network environment. Node not provide constant link between neighbor nodes in MANET. So it does not establish the efficient routing path. Proposed Flat velocity and connection trustworthiness technique (FVCT) to provide a best communication path with trust based link between neighbor mobile nodes in network. Sender node when choose routing path consider cost of routing. It handles lot of injuries like connection loss makes packet drop and packet latency in every transmission. So it provide constant link between mobile nodes to improve throughput and minimize packet latency.

Keywords: Flat velocity and connection trustworthiness technique, Best path allocation.

I.INTRODUCTION

Mobile network is a group of wireless nodes which travel along frequently everywhere and every time lacking of communications. This network is open from predetermined environment, minimizes operation cost with time period [1]. Suitable to free environment of the network, protection intrusion can be potential. Mobile network is extremely susceptible to different communication intrusion. These intrusion is kind of denial of service intrusion. Holing attack is capable to modify its characteristics truthful node to an intrusion [2]. Those nodes are losses the packet information partly otherwise completely forward packets among intermediate nodes to target node and therefore finally it damage the characteristics of a network. Identification of intrusion is not easy since it can modify into the truthful node following losing the information.

Intruder losses a few quantity of packet, it is significant to differentiate is it intruder or any other network problems such network blocking. Therefore, this is vital to identify and eliminate the attack from the network environment. It presents two schemes depending on fake response add up and Trusty connection [3]. Fake responses add up is used to identify and eliminate intrusion through the procedure of route organization. Fake response added on the basis of request and reply message packets. Trusty connection Link is used to secure the well-known route. Intrusion can alter true state to misbehaving state subsequent to the route recognized and throughout the transmission starts with using trusty connection, confirm connection among two neighbouring nodes surrounded by the well-known route [4]. Based on connection and packets shared along that connection among sender and destination nodes, trusty node easy to find be attacker node in network.

Rest part of the paper is constructed as given below. Part II indicates a related works. In Part III, Proposed description about Flat velocity and connection trustworthiness technique (FVCT) attains efficient routing path with smooth node velocity and trusty connection between nodes with minimum energy usage. Part IV provides simulation performance report monitor obtained under various metrics. Finally Part V concludes the paper with future Enhancement.

II.RELATED WORKS

Ganganath,et[5]present minimum distance path finding do not always assurance lesser energy usage of mobile nodes. It presents novel technique to create energy well-organized paths on irregular terrain with a well-known energy price representation for mobile nodes. Network environment are denoted using grid based altitude map. This scheme, the energy charges for packet transmission through a specified node on heuristic energy charge calculation from the present position to the target node. The proposed heuristic energy charge method constructs it possible to create wind like route pattern on vertical hills less than the power boundaries of the mobile nodes. Consequently, the present method should detect physically possible energy-efficiency.

Henan Li, et al., [6] present a novel Optimized Link State Routing scheme indicates as SMLR OLSR-Smooth Mobility and Link Reliability based OLSR. It is constructed on the basis of a prudentially intended SMS CR-Semi-Markov Smooth and Complexity Restricted mobility model that complies suitably with realistic node characteristics and is naturally used for dependability enhanced MPR-Multi Point Relay collection in SMLR OLSR. Experimental output indicates that the present method ensure correct

presentation investigation; also obtain higher MPR lifespan and minimum traffic rate.

Shaik Mazhar Hussain1, et al., [7] proposed various latency that is concerned when communication allowing for various paths, hops and various charge with necessary arithmetical calculations and situation that establish to be sufficient for fulfilling difficulty of QOS-quality of service such finding a path with lesser packet latency. At the same time the remaining routes want to be utilizing to ignore the packet delivery rate to get dishonoured. In Packetizing is worn that improves the efficiency and effectiveness of a network. Present a method that can certify lesser latency among the communicating metrics should vary.

Achraf Kessab, et al., [8] Proposed to evaluate the amount of HSs-hybrid satellite gateway stations in a representative group. Technique for the global route finding method and for the satellite opening collection is presented. Develop the priority thickness process of the end-to-end propagation delays considering GEO-geostationary; MEO-medium then LEO-lesser earth orbits satellite process. Experimental output consider various average density of satellite HSs allow a sender node to discover a trade-off among the charges induce by the count of HSs in the mobile environment, the used satellite orbits and the obtained point to point propagation latency.

Rath, et al., [9] present dependable network layer rule with filtered latency and power for MANET-Mobile Adhoc Network depending on the notion of AODV-Adhoc On demand Distance Vector Routing. Though different those kind of rules are residential for MANET mobile network communication, except this scheme is various in a path that it estimates the fixed range as a process of Power usage, Bounded latency and Packet dispensation rate of the node to be chooses for packet transmission towards target node in a traffic managing way in its place of the minimum distance route and next a cross layer scheme is launched with handshaking among data link layer and network layer to minimize the overload of network layer when path discovery by minimizing power usage.

Bannered, et al., [10] proposed MANET is fitting for provisional message connections. Major difficulties in this type of networks are to discover a route among the communication end node that are irritated from side to side the node velocity. Latest on demand power managing transmission condition for mobile network. It is depends on swarm aptitude and particularly on the ant colony based packet transmission. This method tries to chart the result ability of swarms to arithmetical and manufacturing issues.

III.OVERVIEW OF PROPOSED SCHEME

Present flat velocity and connection trustiness technique in mobile ad hoc network. To make network as efficient one for packet transmission along the path, node travel along network infrequent in various direction, so packet loss is occurred. Packet loss occurred because of unstable connection between routing nodes to overcome this drawback. Propose a FVCT to achieve the constant packet communication among various routing path.

Wrong acknowledgement identifier is implemented to find the misbehaving node characteristics because of unstable connection between sender node and target node. Target node gives a wrong acknowledgement to appeal packet to monitor overload rate when communication is established in that path among sender node and target node. The Original connection method is applied for path security over a node which modifies their characteristics truthful node to hateful after the route allocated and packet transmission started.

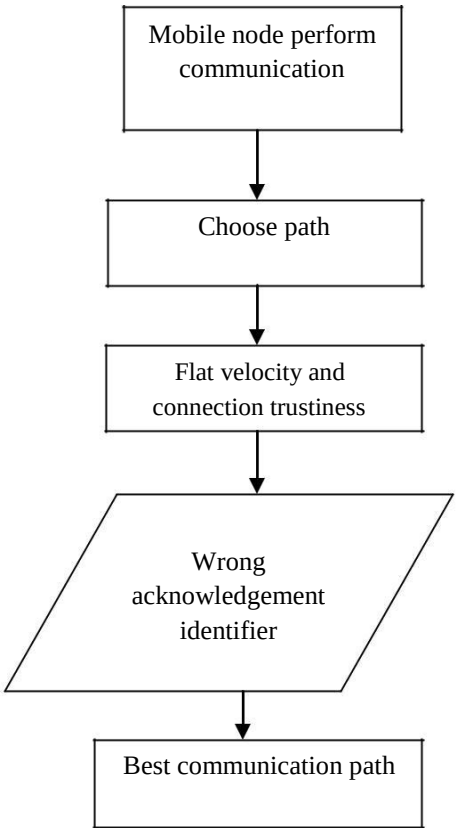

Figure 1: Block Diagram of Flat velocity and connection trustiness

Figure 1 show the Block Diagram of Flat velocity and connection trustiness. Mobile nodes have sender and target node to perform communication. It only select trusty node for packet sharing. Whether any wrong

actknowledgement signal is identified may affect the entire communication. Trusty node easy way to find the wrong acknowledgement signals.

3.1 Sender choose routing path

Sender node difficult to select the communication paths, since it transmit data packet at frequently with high speed for node travelling around mobile network environment. Situation collection of a message packet travel along the source node to target node. It initially tests by sample request packet forwarded to particular intermediate node with abnormal speed. The initial time also noted before packet transmission start, it travels along various directions.

Correct way to travel nodes in constant velocity, and that its sensible trajectory is authorized to a little deviate. In order to understand constant changeover from source node to target node, differentiate the result of those nodes behaviour. Packet delivery rate of each node transmission is analyzed. Network based on that output condition, easy to provide best path with support of acknowledgement packet from target node in network.

Smooth velocity allocation is important one for every node communication, then implements the flat velocity technique need to enhance packet transmission between source nodes to target node in particular routing path. All paths have connection but which one is trusty or fake depending on the behaviour of nodes. So, difficult to identifying smooth velocity nodes in routing path.

To verify true connection in updated mobile node position takes so much of energy. This process is repeated for every time, it not end till reaches the best routing path. Resource utilization is higher in every time, to perform communication with maximum energy used. It reduce the transmission efficiency, node connection makes the sometimes failure for packet transmission.

3.2 Flat velocity and connection trustiness technique

In FVCT method mainly focus the sooth speed for node movement at various direction from left to right, right to left, up to down and down to up at different locations, that not fix at constant point, it travels around coverage range of entire network environment. So transmission speed is varied with size of packet forwarded from sender node to target node in network. Connection trustiness focuses the node current location they are absorbed and upload that information to next neighbor node. If any connection get damaged for node moves out of coverage range. Where is best routing paths derived as given below

The Original connection is used to check the adjacency of straight linked node surrounded by the choose route for packet transmission among sender node to target node. Depending on the grouping takes time period with security level. Whether modifies its characteristics, a best node can alter its position after the route find. Therefore, Trusty connection is used for cross-checking with route verification reason. The Trustiness connection is proceeding among each directly linked node within the required route. Security is vital for message; it is applied to obtain dependability of the network. Trusty connection operates into dual parts Link verification executes in between every adjacent node surrounded by the identified route. One mobile node is source and another mobile node is target node. Best communication path is recognized among sender node and target node. Where is initial energy, is total energy consumption

Flat velocity and connection trustiness algorithm

Step 1: Generate efficient source and target node.

Step 2: For node check Connection between remaining nodes.

Step 3: if {Node==trusty connection}

.

Step 4: Sender establish connection to target node.

Step 5: starts to broadcast data packets.

Step 6: else.

Step 7: if {Node==fake connection}

Step 8: Connection is damaged.

Step 9: Ignore that connection.

Step 10: End if.

Step 11: End for.

3.3 Wrong Acknowledgement Identifier

It influences the presentation of network these kinds of malicious nodes creates over load by forwarding wrong acknowledgement signal to the sender. These acknowledgements referred as wrong acknowledgement. That acknowledgement data is captured from receiver node. Identification of a misbehaving node is based on a quantity of wrong acknowledgement packet captured from a target node in a routing path. Identification of a malicious

Node is done during the route organization through path finding. It makes a decision to list out fake behaviour node else trusty. While a trusty node altering misbehaviour node, then it creates wrong acknowledgement packet is detected that path is poor connection.

The wrong acknowledgment transmitted to all nodes in the network. Buffer count contains a normal node to calculate a amount of packet captured wrong acknowledgement from responding nodes. To count a node in that list, situation is whether the first wrong acknowledgement is identified from the trusty node, it does not insert to fake list. Except that whether quantity of wrong acknowledgement is identified from a node, it should regard as misbehaving and get insert to the fake count.

Packet ID: Packet ID contains mobile node behaviour. Furthermore has node's position and activities are analyzed.

Source ID	Destination ID	Sender choose routing path	Flat velocity	Connection trustiness	Wrong actknowledgement identifier
4	4	3	5	6	4

Figure 2: Proposed FVCT Packet format

In figure 2: the proposed FVCT packet format is shown. Here the source and destination node ID field takes 4 bytes. Third one is Sender choose routing path holds 3 bytes. Initially cluster head monitors cluster member node and its position details are maintained in routing table. In fourth field occupies 5 bytes. Flat velocities provide smooth speed of node movement to perform communication. In fifth occupies 6 bytes, the Connection trustiness technique applied to mobile network, it establish best and trusty link connection among mobile nodes. Last filed is Wrong acknowledgement identifier to reduce energy consumption, carries 4 bytes, to detect acknowledgement from receiver or target node, then poor connection is identified.

VI. Performance Evaluation

A. Simulation Model and Parameters

The proposed CHRT is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 sensor nodes deployed in 1000 meters x 1000 meters square region for 65 milliseconds simulation time. All sensor nodes deployed in random manner among the network. 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 packet overload.

DSDV Destination sequence distance vector routing is used to monitor neighbour node location to obtain smooth velocity of node and efficient connection in mobile network to attain lesser energy consumption with higher Packet delivery ratio. Table 1 shows Simulation setup is Estimation.

Table 1: Simulation Setup

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11g
Radio Range	250m
Simulation Time	90ms
Traffic Source	CBR
Packet Size	150 bytes
Mobility Model	Random Way Point
Protocol	DSDV

Performance Analysis

In simulation to analyzing the following performance parameters are using X graph in ns2.34.

Path Stability Figure 3 shows path stability is established by constant velocity for node with efficient connection when packet transmission period with quantity of packet broadcast, each nodes information's are maintained in routing table it helpful for stabilization. In proposed FVCT scheme path stability is increased compared to existing method SMLR [6].

= *

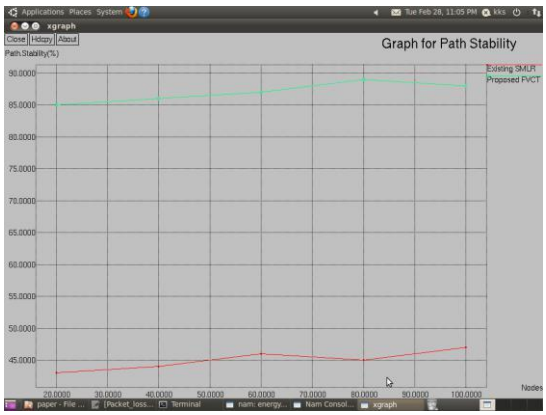

Figure 3: Graph for Nodes vs. Path Stability

Packet Delivery Ratio: Figure 4 shows Packet delivery ratio is measured by packet received from

packet sent in particular rate. Speed of node is constant in sensor network; simulation rate is fixed at 100. In proposed FVCT scheme Packet delivery ratio is better compared to previous method SMLR.

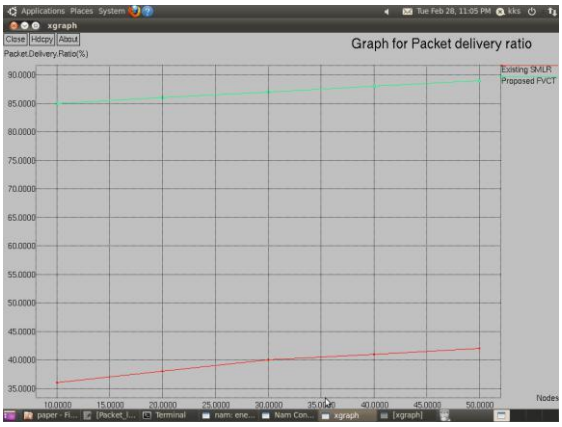

Figure 4: Graph for Nodes vs. Packet Delivery ratio

Energy Consumption: Figure 5 shows energy consumption; evaluate total energy used for starting node to ending node. In proposed FVCT scheme constant velocity of nodes with steady link are used to obtain so energy consumption is reduced compared to previous scheme SMLR.

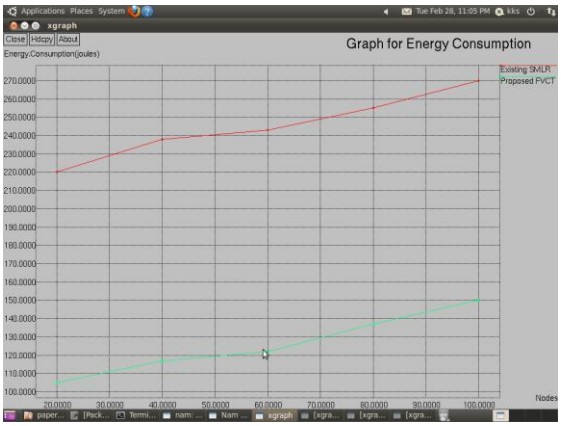

Figure 5: Graph for Nodes vs. Energy Consumption

Packet Loss rate: Figure 6 show that Packet loss of all transmission in network is designed by nodes loss the packet since of data packet traffic so go for flat velocity of node movement, it gives efficient communication. In proposed FVCT scheme Packet loss rate is decreased compared to previous scheme SMLR.

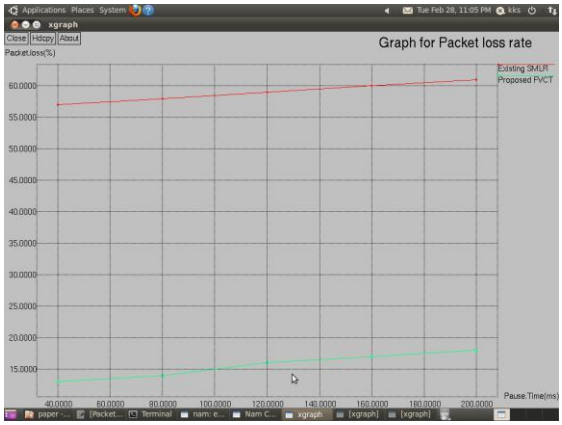

Figure 6: Graph for Pause Time vs. Packet loss rate

V. CONCLUSION

Mobile nodes are free movement in nature with different velocity so connection failure occurred during packet transmission time, nodes are unable to stabilize the connection, also not achieve efficient packet transmission. Present (FVCT) Flat velocity and connection trustiness technique to provide the efficient communication in mobile network, smooth speed of nodes forward data packet in stable connection among sender to destination node. It improves packet delivery ratio, path stability and reduce energy usage, packet loss rate. In future work measure efficiency with unstable node movement to analyze different parameters.

REFERENCES:

[1] Jeron Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester,"An overviw of Mobile Ad-Hoc Networks: Applications and challenges." (July 2004). Journal of Communication Networks, 3,60-66.0.

[2] Shalini Jain, Mohit Jain, Himanshu Kandwal,"Advanced for Detection and Prevention of Co-operative Black and Gray Hole Attack in Mobile Ad-Hoc Networks." International journal of computer Applications (0975-8887) volume 1-No. 7,2010.

[3] A. Kanthe, D. Simunic, R. Prasad ," A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks "International Journal of Computer Application (0975-8887) Volume 53-No.16, September 2012.

[4] G. Wahane, A. Kanthe, D. Simunic,"Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET".IEEE International Conference on Computational Intelligence and Computing Research, 2014.

[5] Ganganath, Nuwan, Chi-Tsun Cheng, and K. Tse Chi. "Finding energy-efficient paths on uneven terrains." Mecatronics (MECATRONICS), 2014

10th France-Japan/8th Europe-Asia Congress on. IEEE, 2014.
[6] Li, Zhinan, and Yinfeng Wu. "Smooth Mobility and Link Reliability based Optimized Link State Routing Scheme for MANETs." IEEE Communications Letters (2017).
[7] Hussain, Shaik Mazhar, et al. "Least delay path estimation routing protocol (LDPERP) with enhanced multimedia transmission through parallel links over heterogeneous MANETS." Research and Development (SCOReD), 2016 IEEE Student Conference on. IEEE, 2016.
[8] Kessab, Achraf, et al. "Optimizing end-to-end propagation delays in hybrid satellite-maritime mobile ad hoc networks." Software, Telecommunications and Computer Networks (SoftCOM), 2016 24th International Conference on. IEEE, 2016.
[9] Rath, Mamata. "Optimized network layer protocol with cross layer handshaking mechanism in MANET." Intelligent Systems and Control (ISCO), 2016 10th International Conference on. IEEE, 2016.
[10] Banerjee, Saptarshi, et al. "Modified Ant Colony Optimization (ACO) based routing protocol for MANET." Computing and Communication (IEMCON), 2015 International Conference and Workshop on. IEEE, 2015.

Author profile

S. Prabu received the B.S.c. degree in computer Science from the Bishop Thorp college, Dharapuram, Bharathiar University ,Coimbatore, India, in Apr 2003, the M.C.A degree in (Computer Application) from the Cherraan's Arts Science college ,Kangayam, Bharathiar University, Coimbatore, India, in April 2006 and the M.Phil degree in Bharathiar University, Bharathiar University, Coimbatore, India, in Nov 2008.His research interests include communication and networks mobile ad-hoc networks, Mobile computing, AI, Network Security . He has about 9 years of teaching experience, since 2017.