ZMDTN: DISTRIBUTED FAULTY NODE DETECTION USING ZONE-BASED MULTI-PATH DELAY TOLERANT NETWORK

S. AMUTHAVALLI[1]
Assistant Professor, Department of Computer Science,
Sri Ramalinga Sowdambigai College of Science and
Commerce, Coimbatore, India.

C. ANTONY METILDA DEVERA[2]
Assistant Professor, Department of Computer
Science,
Bishop Ambrose College,
Coimbatore, India.

S. KAVITHA[3]
Assistant Professor, Department of Computer Science,
Bishop Ambrose College,
Coimbatore, India.

Abstract: Mobile Ad-hoc networks have opened a new measurement in wireless networks. It allows mobile nodes to exchange a message in deficiency of centralized support. Integrating Delay Tolerant Networks (DTN) in MANET has to look elevated issues due to dynamically modifying the topologies (Faulty detection and Scheduling on End-to-End Throughput in Multi-Hop Wireless Networks), small transmission energy and asymmetric links. To address these issues of Faulty detection, in this paper work, proposed a Distributed Networks with Probabilistic Graph Modelling with Authenticated secret Secure Routing using Zone-Based Multi-Path Delay Tolerant Network (ZMDTN) algorithm combines the advantages of proactive and reactive routing. The proposed ZMDTN link state routing topology has certain characteristics, which imposes new demands on the routing protocol. Meanwhile, proposed framework for identifying the traffic alerts generated by specific faulty detection mechanisms in Mobile Nodes (MN). Through Experimental simulations, to validate that the proposed framework achieves significantly better Packet Delivery ratio and Throughput than existing methods of Probabilistic Misbehaviour Detection Schemes.

Keywords: Delay tolerant networks, fault detection, MANET, Multi-path.

I. INTRODUCTION

Wireless networks, whether mobile networks or local area networks (LANs) have rapidly become an indispensable part of our life. By now, the number of wireless phones has superseded that of wired ones. Wireless LANs are routinely used by millions of nomadic users. In today's development, every user wants to remain connected so that the transfer of information and data can be done quickly.

Delay Tolerant Network is totally different approach than frequently linked wired or wireless networks [1]. In DTN, there is no end to end path accessible at several point of time for transmitting data among a pair of source and target node. The communication in DTN is done by developing the characteristic of mobile nodes i.e. mobility, accessible connections, and offered buffer space etc.

The Delay Tolerant Networks play the major role in the circumstances where the paths connecting any pair of nodes could never be attained. In sparse network setting where there are no end to end paths obtainable, like in military battlefields, DTN presents the means to communicate. It does not necessitate any preceding knowledge of networks to promote the bundles from single node to any more. It is based upon the accumulate and carry forward method. In internet where routing means to decide the finest optimal path whereas in DTN routing means to guarantee the packet delivery of collections to target with smallest amount delay incurred.

In MANET, the supporting of packet is done when the connection among end points are already created. It means in MANET, the routes are formed to and from the end mobile nodes then after the promoting is done from origin to target. Whereas, DTN have no paths are formerly created for forwarding. The packets are routed by relaying the packets to obtainable suitable nodes.

This paper focuses a distributed Faulty Node Detection in Delay Tolerant Network routing algorithm which can be used for multicasting in DTN, which improved exploits the network resources and promises the delivery of packet with least possible delay acquired. The multicasting refers to forwarding packets to a set of nodes with recognized path towards each other node throughout some intermediate nodes. In DTN, the routes are not previously established. Packet for still a particular target may travel during multiple relay nodes to promise the delivery at earliest. Multicasting [2-3] in DTN is complete in the approach that origin node produce the packet and establish replicating it to other mobile nodes coming in contact, the nodes getting the packet also additional replicate it to other mobile nodes to make it attain the group of targets. The packet does not contain target as set of nodes but the address of nodes particularly because nodes remain changing their locations and so their corresponding groups.

The objective of this paper is trying to discover DTN multi-path routing focuses on the selection of nodes to form a path from a message source to the destination in the network. Meanwhile, to calculate the shortest K Shortest path routing is to find the highest secure connection probability path between any given source-to-destination pair in a distributed way.

The features of the proposed system are as follows:

- It decreases network collision and allows flexible operation.
- To minimize the computational and transmission overhead by exploiting the bundle buffering characteristics.

II. RELATED WORK

(*P. Hui, J. Crowcroft, and E. Yoneki*, **2011**) [4] authors exploited two social and structural measures, specifically centrality and community, using real human mobility suggestions. They designed and evaluated BUBBLE, a novel social-based forwarding algorithm that exploits the abovementioned measures to improve packet delivery performance. Next, they empirically showed that BUBBLE can considerably recover forwarding performance evaluated to an amount of before proposed algorithms comprising the standard social-based forwarding SimBet algorithm and history-based PROPHET algorithm.

(*E. Ayday and F. Fekri*, **2012**) [5] authors developed an iterative malicious node detection mechanism for DTNs submitted as ITRM. Their technique is a graph-based iterative algorithm forced by the past success of packet passing techniques for decoding low-density parity-check codes above bipartite graphs. Relating ITRM to DTNs for different mobility models, they examined that the iterative reputation management scheme is extreme more efficient than well-known status management methods such as the Bayesian framework and EigenTrust. Additionally, they concluded that the scheme offers high data accessibility and packet-delivery ratio with small delay in DTNs under different adversary attacks which effort together challenge the faith and detection technique and the packet delivery protocol.

(*H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao*, **2014**) [6] authors investigated the malicious and egotistical actions signified a serious threat besides routing in delay/disruption tolerant networks (DTNs). Suitable to the distinctive network characteristics, manipulative a misbehavior detection scheme in DTN is observed as a big challenge. They proposed iTrust, a probabilistic misbehavior detection scheme, for protected DTN routing toward competent faith establishment. The fundamental idea of iTrust is initiated an occasionally available Trusted Authority (TA) to judge the node’s performance based on the together routing proofs and probabilistically checking. Their model iTrust as the examination game and use game theoretical analysis to express that, by setting a suitable examination probability, TA could guarantee the security of DTN routing at a decreased cost.

(*Wei*, et.al, **2015**) [7] authors discussed the network jamming from a neighborhood perspective and take it into account the plan of packet forwarding algorithms. They initially promote a novel distributed community detection method, which could path the development of communities. Based on the recognized communities, they developed a congestion prevention mechanism to redirect the load absent from the congested regions to the different custodians and additionally presented a congestion-aware packet forwarding algorithm where packets can circumvent being broadcasted to the congested mobile nodes. They finally calculated the efficiency of distributed community detection and congestion-aware packet promoting through the extensive real-trace driven simulations

(*L. Galluccio, B. Lorenzo, and S. Glisic*, **2016**) [8] authors proposed a Delay-tolerant networks (DTNs) consists of nodes moving approximately and rarely coming into every other's proximity. During the incomplete proximity time, mobile nodes can replace data; this cans consequence in an especially slow data distribution procedure that is regularly directed by a replication-based method. They represented a feasible solution to create transmission more dependable, therefore delaying the establishment of the fault recovery process, depending on the amount of nodes, targets, and the time. Furthermore, they also proposed to develop an additional characteristic in data multicasting, i.e., socially aided data distribution, where the message dissemination process is not slightly epidemic, but quite developed the essential sociality of users and their interests to decrease the packet delivery overhead and speed up the multicast procedure. Further exclusively, they considered a process where users are not observed as individual members of the network but can be combined into groups sharing interests, and their sociality assists the data dissemination process.

(*Wenjie Li, Laura Galluccio, Francesca Bassi, and Michel Kieffer*, **2018**) [9] authors developed a completely distributed and simply implementable approach to permit each DTN node to quickly recognize whether its sensors are creating faulty data. The dynamical performance of the proposed algorithm is approximated by several continuous-time condition equations, whose equilibrium is characterized. The presence of faulty nodes, difficult to perturb the faulty node detection process, is also taken into account. Detection and false alarm rates are estimated by comparing both theoretical and simulation results.

III. RESEARCH METHODOLOGY

In this paper, proposed method accepts the simulation parameters as input which contains the NS2.34 simulation where the optimal Zone based distributed Faulty Node Detection in multi-path Delay Tolerant Network is applied to the mobile adhoc network. This overall proposed flow diagram in figure 1 follows a DTN routing procedure form start to end state. Every mobile node of these networks performs as routers and obtains part in finding and preservation of routes to additional mobile nodes in the network. This characteristic presents a huge challenge to intend of a routing system because connection bandwidth is extremely incomplete and the network topology modifies as users. This work examines the performance of accessible conventional routing algorithms and proposes and implements a novel multi-path DTN routing approach for wireless networks.

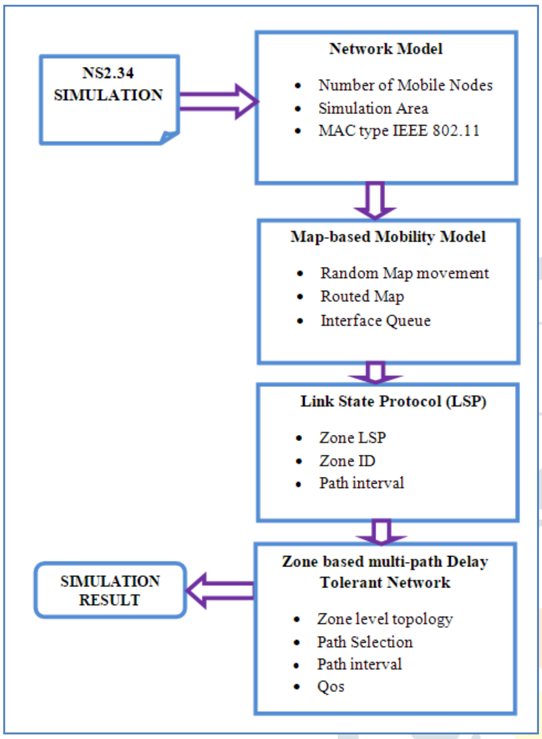

Figure 1: Proposed Flow diagram

A. *NETWORK MODEL*

In the network mode, considers a wireless network consisting of *N* nodes, indexed by 1, …, *N*. Assume all transmissions are over the similar frequency band. Expect for simplicity each mobile period is of single symbol interval and all nodes are perfectly coordinated over each frame of *M* slots. Let the binary on-off duplex mask of node *n* over periods 1 through *M* be denoted by $P_n = [p_{1n}, \ldots, p_{Mn}]^T$. During period *m*, node *n* may transmit a symbol if $p_{mn} = 1$, whereas if $p_{mn} = 0$, the node listens to the channel and emits no energy.

B. *MAP-BASED MOBILITY MODEL*

Map-based mobility model is that forces Mobile Nodes (*MN*) to journey to the boundary of the model area before altering path and velocity. This representation does not experience from the compactness effect in the middle of the framework space that Random Waypoint model does. In this representation, map based mobility chooses a random track in which to move parallel to the random walk mobility Model. A MN travels to the edge of the simulation area in the corresponding direction. One time the process simulation margin is attained, the mobile node pause for a particular time, choose a different sharp direction (between 0 and 360 degrees) and maintains the process.

The map mobility movement model directs the technique nodes travel in the simulation. It provides mobile coordinates, speeds and pause times for the nodes.

A different movement models obtainable in map based mobility. Some of them are discussed here.

- Random Waypoint
- Map Based Movement Model

Random Waypoint: In this model, mobile nodes move randomly in subjective way. There is no exacting mechanism following the node mobility. If a few changes in node orientation and/or speed the random way point contains pause times among on it. Mobile nodes begin from one position and then journey randomly in several directions.

Map Based Movement Model: In this model, there is structured map and node moves on the source of that map. The simulator discharge includes three map-based association models.

C. *LINK STATE PROTOCOL*

The link-state protocol (LSP) is essential functionality is to determine neighbors and distribute together topology and name prefix information. Such functionality might appear to be straight-forward to plan and realize. Nevertheless, LSP uses Networking attention and packets to broadcast routing updates, the aim have to move away from the recognizable notions of approaching messages to known network address (i.e., some mobile node can send several message to a few other mobile node). The link state protocol model, mobile node use the shortest path from all available paths, shortest available path is chosen on the basis of Dijkastra algorithm that is applied as backend. Map data can also contain Points of Interest (POIs). The searching method is based on maintaining a global priority queue of mobile nodes with priorities equal to their distances from the source node. In every iteration the algorithm expands the node with the shortest distance and updates distances to all reachable nodes. The distance calculation using Euclidean distance as follows,

$$Dist(mn) = \sqrt{Mn(i)_{xd} - Mn(i+1)_{xd}{}^2 + Mn(i)_{yd} - Mn(i+1)_{yd}{}^2} \qquad eqn.(1)$$

Where, *Mn* is the mobile node assignment, *xd* is the nodes *x*-coordinates, *yd* is the nodes y- coordinates.

Algorithm 1: Dijkstra's Path Search algorithm
Input: Graph *G*, Distance *Dt*, source *s*, *Destination D.*
Output: Updates the shortest distance.

```
Step 1: Initialize distance d[s] $\leftarrow$ 0.
Step 2: for all $Mn$ $mn \in MN$ do
        d[$mn$] $\leftarrow \infty$
        Q $\leftarrow$ {$MN$}
Step 3: while Q $\neq \Phi$ do
        $u \leftarrow$ Extract minimum($Q$)
        for all mobile nodes $mn \in u.Adjecencylist$ do
            if Dist[$mn$] > Dist [u]+ Dist (u,v) then
                $d[v] \leftarrow d[u]+Dist(u,v)$
Step 4: End process when all nodes have been $mn$ visited.
```

D. *ZONE-BASED MULTI-PATH DELAY TOLERANT NETWORK (ZMDTN)*

The ZMDTN algorithm predicts the Faulty Node Detection in mobile adhoc network. In the detection method, each mobile node in the network, that monitors the performance of its neighbors and leading detecting any anomalous action by some of its neighbors invokes a distributed algorithm to determine whether the node performs abnormally is indeed malicious. This algorithm works through collaboration of some security components that are present in every node in the networks. These components as follows: (i) Reliability State, (iii) Monitoring Node. The functions of these components are described below.

Reliability State: In this state, a node raises a majority consensus algorithm amongst the neighbors of a node that has been suspected to be faulty or malicious. On being activated by its reliability state, the mobile node that has assumed some malicious activity by individual of its neighbors disputes the suspicious node to confirm its behavior as observed by all of its neighbors. The accused (suspected) mobile node on receiving the challenge reacts by accepting the packet and sending a authenticate behavior packet to all of its neighbors. The neighbors react by sending the experimental value of the degree of maliciousness of the accused node. The faulty node calculates the group's faith in its performance using the received values and transmits the computed group-faith beside with the received responses to all the neighbors. The packets are also time-marked so as to stop replay faults. For calculating group reliability value from the expected responses, any consensus-based method can be used. In the proposed method, the dissimilarity of the complete reliability values and the standard degree of maliciousness of the majority of the respondents (neighbors) has been taken as the absolute reliability value of the mobile node.

Monitoring Node: The monitoring node is answerable for confirming the rightness of the group reliability certificate received, caching them, and modernizing the global faith state (table) of the mobile node for which it has established a new group certificate (from the neighbors of a suspected node). While confirming the correctness, the monitoring node must ensure whether the response from each neighbor node has been properly considered in calculating the group-faith by the suspected node, and the messages have-not been tampered with.

Algorithm 2: Zone-Based Multi-Path Delay Tolerant Network Algorithm

```
Step 1: A source node needs a route to destination the protocol starts mobility path discovery. During path discovery, source node broadcast RREQ packets through adjacent nodes.
Step 2: While receiving the RREQ packet each node update their routing table (RT)
Step 3: Compare both Adjacent List (AL) and compute the number of frequent neighbor nodes present between sources to destination
        For $k$=0; $k$<amount of source neighbors; $k$++
        For $z$=0; $z$< amount of target neighbors;$z$++
            If (ZMDTN_soruce(k) = ZMDTN _targe(z))
            Regularnode++;
Step 4: Initialize single hop neighbors can reach target node with maximum of 3 hop and minimum of 1 hop. If maximum target count exceeds 3 then target node and their previous hop may be the faulty node.
Step 5: If $targetnodecount$ > $nodecountthresh$ then declare the target node and their previous hop nodes are faulty nodes.
Step 6: Send faulty node announcement message to all nodes.
Step 7: Any node receives attacks announcement message it removes attacker node id from its neighbor table and Routing Table.
```

IV. PERFORMANCE EVALUATION

The proposed work considers an N number of nodes in multi-hop DTN wireless network, with nodes randomly deployed in a 1000 m x 1000 m area. The source node and destination nodes of each session are randomly selected, with the route between the shortest path routes. The proposed ZMDTN method is compared to the existing misbehaving nodes aim at disrupting network operations by causing congestion along paths, unreliable packet delivery, or erroneous data delivery [5].

Packet delivery Ratio (PDR): the ratio of the data packets distributed to the target nodes to those produced by the Constant Bit Rate (CBR) sources. The PDR demonstrates how successful a protocol executes delivering packets from origin to target. The higher for the value give use the improved results. This metric differentiates both the unity and rightness of the routing protocol also dependability of routing protocol by providing its efficiency.

PDR is the fraction of the amount of data packets acknowledged by the target node to the amount of data packets sent by the origin mobile node. It can be assessed in terms of percentage (%). This constraint is also called "achievement rate of the protocols", and is illustrated as follows:

$$\boldsymbol{PDR} = \left(\frac{\boldsymbol{SendPacketno}}{\boldsymbol{Receivepacketno}}\right) \times \mathbf{100}$$

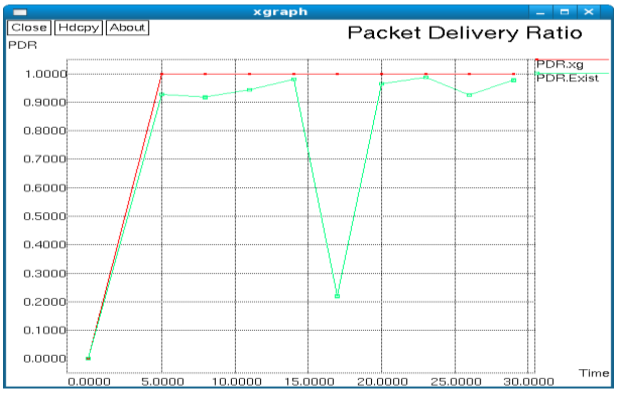

Figure 2: Comparison of PDR

Throughput: It is the relation of the whole quantity of data that attains a destination from an origin node to the time it obtains for the receiver to obtain the most recent packet is referred to as throughput. It is expressed in bits per second or packets per second. It is the standard rate of successful packet delivery over a communication channel. This data may be distributed over a physical or consistent link, or pass through a positive network node.

$$\boldsymbol{Th} = \frac{\boldsymbol{R}}{\boldsymbol{Time}}$$

Where *Th* is the throughput, *R* is the amount of requests that are proficient by the system, and Time indicates the whole time of system examination.

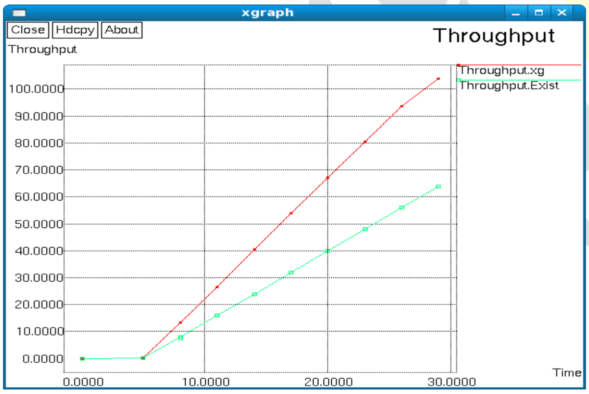

Figure 3: Comparison of Throughput

V. CONCLUSION

In this paper designed, implemented and evaluated implementation of Zone-Based Multi-Path Delay Tolerant Network (ZMDTN) in wireless adhoc network. The proposed ZMDTN algorithm implemented in the wireless application which consists of two important methods (i) Link State protocol and multi-path selection. The proposed links stage routing path communicates wirelessly using the IEEE 802.11b technology exclusive of any assist infrastructure. The main algorithm implemented in this framework was the ZMDTN algorithm, which consists of two important mechanisms; link stage Dijkstra's algorithm (*K* shortest path routing) and zone based multi-path routing. Since the ZMDTN algorithm controls completely based on origin routing and on-demand procedure, it has been chosen as the link stage routing topology to be executed and tested for wireless ad hoc simulation differentiate by an origin on-demand conversation among nodes in a mobile ad hoc network.

REFERENCES

[1] Cerf, Vinton, et al. Delay-tolerant networking architecture. RFC 4838, April, 2007

[2] Santiago, Jos, Augusto Casaca, and Paulo Rogrio Pereira, "Multicast in Delay Tolerant Networks Using Probabilities and Mobility Information." Ad Hoc & Sensor Wireless Networks 7.1-2 (2009): 51-68.

[3] Zhao, Wenrui, Mostafa Ammar, and Ellen Zegura, "Multicasting in delay tolerant networks: semantic models and routing algorithms", Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking. ACM, 2005.

[4] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE rap: Social-based forwarding in delay-tolerant networks," IEEE Trans. Mobile Comput., vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[5] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," IEEE Trans. Mobile Comput., vol. 11, no. 9, pp. 1514–1531, Sep. 2012.

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.

[7] K. Wei, M. Dong, J. Weng, G. Shi, K. Ota, and K. Xu, "Congestionaware message forwarding in delay tolerant networks: A community perspective," Concurrency Comput.: Practice Experience, vol. 27, no. 18, pp. 5722–5734, 2015.

[8] L. Galluccio, B. Lorenzo, and S. Glisic, "Sociality-aided new adaptive infection recovery schemes for multicast DTNs", IEEE Trans. Veh. Tech., vol. 65, no. 5, pp. 3360–3376, May 2016.

[9] Wenjie Li, Laura Galluccio, Francesca Bassi, and Michel Kieffer, "Distributed Faulty Node Detection in Delay Tolerant Networks: Design and Analysis", IEEE transactions on mobile computing, VOL. 17, NO. 4, APRIL 2018.