Self Diagnosing and Fault Evacuation Framework for Ad-Hoc Network

Karthick Raghunath K. M., Vallimayil A., and Mala@ Aarthy M. P. A.

***Abstract*—Ad hoc networks are new wireless communication paradigm for mobile hosts. Ad hoc network does not pose any fixed infrastructure such as mobile switching centers or base stations. Since nodes in ad hoc networks are dynamic in nature, very much prone to failures due to various faults. In our paper, we propose a systematical, Self-diagnosing and Fault evacuation framework inorder to minimize node failure, congestion failure and link failure in Ad hoc networks. This framework is mainly designated to concentrate on the cause that brings failure to the routing session in the network. In this context, Dynamic MANET Ondemand (DYMO) routing protocol is a reactive protocol and formulated to handle a wide variety of mobility patterns by dynamically determining routes on-demand. This paper also presents a comparative analysis of various impacts of framework in Ad-Hoc Network. The goal of this paper is to help researchers, working in this area to construct better working environment with better parameterization.**

***Index Terms*—Ad hoc network, DYMO, fault tolerance, self-diagnosing, fault evacuation.**

I. Introduction

In information and communication world, a network is a series of interconnected nodes by communication paths. Several networks can be interconnected with other networks and contain sub networks. Ad hoc network [1] devices could establish connections with each other without usage of access points in which the nodes are mobile and could form arbitrary topologies. As result some nodes could not directly connect to each other due to the mobility conditions or limited reception range of wireless antennas. For such node, packets should be transmitted through other nodes with well defined routing protocol. Since the routing protocol plays a major role, it should be self-configuring, self-healing and should dynamically reconfigure routes after departure of existing nodes and joining of new nodes into the network. Infrastructure-less networks are becoming more popular with the increased prevalence of wireless networking technology. A significant challenge faced by this infrastructure-less networks is that it is not provided with standard protocol. Here, we analyze our Self-Diagnosing and Fault Evacuation (SF) Framework with one of most recent popular routing protocol called Dynamic MANET Ondemand routing protocol (DYMO) [2]. This review mainly deals with the way in which the solutions differ in Ad-Hoc networks due to various faults, and the main contributions of SF framework and conclusions.

Manuscript received Jun 18, 2012; revised July 10, 2012.

The authors are with the ME (Pervasive Computing Technologies), Anna University Of Technology, Tiruchirapalli-620024,India.

II. DYMO

DYMO [2] routing protocol enables reactive, multihop unicast routing between active DYMO routers. The basic operations of the DYMO protocol are

- Route discovery
- Route maintenance

Before this, route discovery and maintenance, let us discuss about the key operations of these DYMO routing protocol: RREQ, RREP, RERR [3].

- *ROUTE REQUEST* (RREQ): A RREQ [2] message is issued to discover a valid route or routing path to a particular destination address, called the RREQ TargetNode. When a DYMO router processes a RREQ, it learns routing information on how to reach the RREQ Originator Node.
- *ROUTE REPLY* (RREP): A RREP [2] message is used to disseminate routing information about the RREP Originator Node, to the RREP TargetNode and the DYMO routers between them
- *ROUTE ERROR* (RERR): A RERR [2] message is used to indicate that a DYMO router does not have forwarding route to one or more particular destinations.

A. Route Discovery

During route discovery, the originator's DYMO router initiates dissemination of a Route Request (RREQ) throughout the network to find a route to the target's DYMO router. During this hop-by-hop dissemination process, each intermediate DYMO router records a route to the originator. When the target's DYMO router receives the RREQ, it responds with a Route Reply (RREP) sent hop-by-hop toward the originator. Each intermediate DYMO router that receives the RREP creates a route to the target, and then the RREP is unicast hop-by-hop towards the originator. When the originator's DYMO router receives the RREP, routes then have been established between the originating DYMO router and the target DYMO router in both directions.

B. Route Maintenance

Route maintenance consists of two operations. In order to preserve routes in use, DYMO routers extend route lifetimes upon successfully forwarding a packet. In order to react to changes in the network topology, DYMO routers monitor links over which traffic is flowing. When a data packet is received for forwarding and the current route is broken/unknown, then the status of broken/unknown route is notified. A Route Error (RERR) is sent toward the source DYMO router to indicate the current route to a particular destination is invalid or missing. When the source' DYMO router receives the RERR, it deletes the route. If the source' DYMO router later receives a packet for forwarding to the

same destination, it need to perform route discovery again for that destination. DYMO uses sequence numbers to ensure loop freedom. Fig. 1 depicts the mechanism of DYMO.

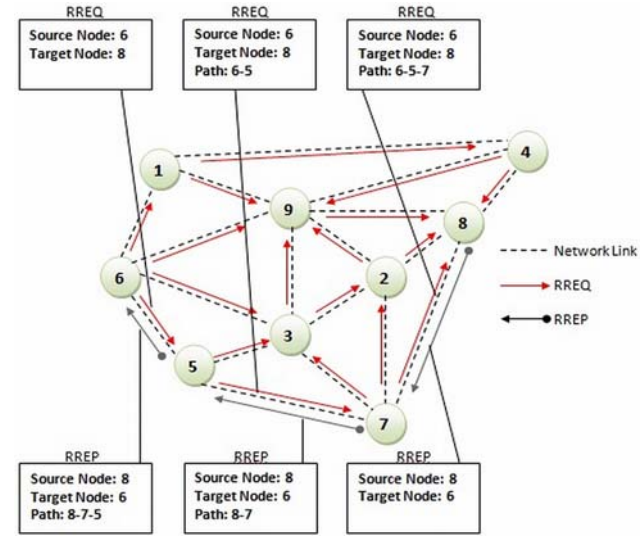

Fig. 1. Mechanism of DYMO routing protocol [2].

III. Self-Diagnosing and Fault Evacuation Framework (SF) Framework

The SF framework comprises three modules: Self-Diagnosing management, Fault Evacuation Management and the Refinement/Impeccable phase. The coordination of these three modules is depicted in Fig. 2.

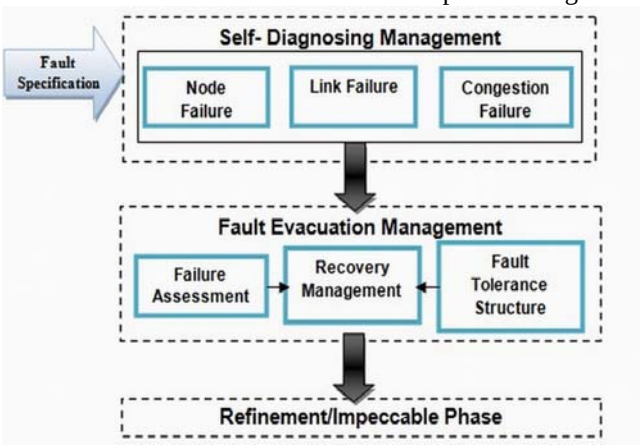

Fig. 2. SF framework.

A. Self-Diagnosing Management

In the Self-Diagnosing management module, remarkable fault specifications such as link failure, node failure, and congestion failure are taken into consideration gathered during network communication on the expected faults and their estimated frequencies. It also provides valuable information regarding the resources that need to be fault tolerant.

Mechanism: Self-diagnosis is prone to error and might be potentially dangerous if inappropriate decisions are made on the basis of a misdiagnosis within the network. So SF framework is aware of diagnosing the faults with respected to the fault specifications, which are predefined by the system manager. The module exhibits the following sequential order to diagnose the faults during routing.

1) Special functional module

Once the routing protocols establish the optimal routing path between the source and target node, the self diagnosing management activates the special functional module that are provided to each of the network node. On the commencement of communication, each activated special functional module diagnoses the established routing path and identifies the existing failures. The gathered information is accounted periodically by functional module to its associated node. Moreover each functional module store and update the resource data as a checkpoint. This stored data are restored later, on the occasion of fault occurrence.

2) Fault disclosing act

It mainly deals with the detection of faulty behavioral nature of the system or network. It also carries the task of disclosing major and minor faults with respect to the fault specifications such as node failure due to energy depletion or hardware damages, link failure due to dynamic nature of the network and congestion failure.

B. Fault Evacuation Management

The Fault Evacuation management consists of the following:

1) Failure assessment

It refers with the basic cause of the failure and deduce the recovery alternatives that leads to the optimize use of resource. A set of deduced recovery alternative are handled to the recovery management. For example it evaluates the data loss due to congestion or link failure and prepares a recovery plan to recover the lost data.

2) Fault tolerance (FT) structure

This structure provides the set of job/task. This job/task eliminates the fault effect and provides the solutions to restore the network to its normal operation. The job/task provided according to the recovery alternatives deduced by failure assessment.

3) Recovery management

This management evacuates the faults and ensures the fault tolerance capability during the communication.

C. Refinement/Impeccable Phase

This phase enables the faulty network to fault free network and enable the network self configurable based on the network changes [3].

IV. System Model and Definition

In this section we apply our SF Framework to Ad-Hoc network model. We consider a homogeneous network in terms of energy and node capabilities. Here each node is provided with a special functional module called Relay-Checkpoint Module (RCM). Once the routing protocol establishes the routing path, each node that involve in the communication triggers their integrated RCM. Fig. 3 depicts our system model.

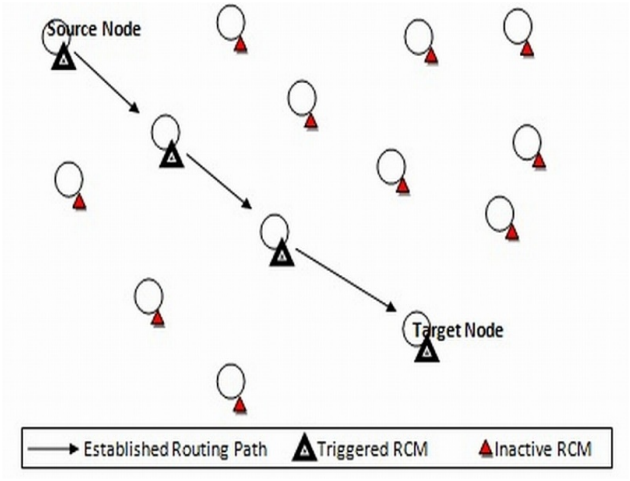

Fig. 3. SF framework assisted Ad-Hoc network.

In Ad-Hoc network, we denote the source node by S_1 ,…, S_n and other nodes by N_1 ,…, N_n. We define $G_{i,j}$ as generated source to be send to the target node, where j denotes the set of source packet from a source node S_i.

Trigger RCM_i where i=1,2,...
Start diagnose //In established routing path//
do
Upon **recv** ($G_{i,j}$)
Replicate and Save ($G_{i,j}$) //obtained from source node//
AddTo (IS_n)
Upon **recv** (set of $NodeID_i$) //Including Source and target node//
AddTo (IS_n)
Upon **recv** (set of $LinkID_i$) //incoming and outgoing link//
AddTo (IS_n)
Upon **recv** (set of $Energy_{level}$)
AddTo (IS_n)
Send (IS_n) **To** Associated node
Until ("The target node receives the resources")

Fig. 4. Primary functionality of RCM

.

The pseudo code of Fig. 4, depicts the primary functionality of each RCM is, gathering of set of information (IS_n) regarding established routing path such as Node ID and energy level of the associated node that involves in the communication, incoming and outgoing Link ID of their own associated node.

TABLE I: RCM INFORMATION SET.

Node IDs	Active communicative node	In-active neighbour node
	$NodeID_1$…$NodeID_n$	$NodeID_1$…$NodeID_n$
Nodes' Energy level in the established routing path.	Set of E(t)→ energy level at regular time interval during communication.	
Incoming and outgoing Link IDs of the associated node in the established routing path	Incoming LinkID, Outgoing LinkID	
Data	Replicate the data of source node and stores	

Each RCM gathers available inactive neighbour nodes ID and their energy level. RCM gathers only single hop neighbour node information that is within the associated nodes' transmission range. The RCM can be invoked to gather IS_n periodically e.g., every T seconds during communication. The secondary functionality of these RCM is to relay the gathered IS_n to their associated node periodically and storing the replicated data [4] of source node. RCM also plays a vital role in the fault evacuation management. See Table I for the information contents of RCM.

V. IMPLEMENTATION OF SF FRAMEWORK

A. Self-Diagnosing and Fault Evacuation

The self-diagnosing management of SF Framework achieves the identification of fault by RCM. Each RCM gathers and provide the information set (IS_n) attributes to their associated nodes.

1) Node failure identification

To predict the node failure we define a conditional percentage threshold $a < \mu < b \ \forall \ N_n, S_n$, such that remaining energy level reaches below μ then the node becomes incapable of participating in routing session.

Recovery mechanism: During communication, the energy level of each node is examined by its integrated RCM at regular time interval (t). After the failure assessment, fault structure imposes its alternative recovery method to the identified fault node. This method eliminates the fault effect by choosing a nearest optimal node (N_{n+1}) (threshold value greater then μ) to involve in the communication. Once the new node involves in communication, it triggers its RCM. RCM of new node gathers the (IS_n) for further communication.

2) Link failure identification

Since Ad-hoc network are dynamic, position of the nodes cannot be static. Therefore link failure is a common issue in Ad-Hoc network [5]. Due to the dynamic nature of the nodes, present link status between the source node and target node faces extreme changes. This action leads to the link failure. To identify the link failure, FT structure considers the LinkID for each link that has been established between the nodes by routing protocol. The Link failure status can be identified by the missing LinkID in the LinkID attribute list in RCM information set (IS_n) at regular periodic update.

Recovery: During transmission flow, the upstream or downstream links of a specified node is marked as weak link, if its transmission data quality rate and receiving data quality rate, fades below the Extremely Low Data Rate *(ELDR)*, ranges from 300 bits/s to 3 kbits/s. Such a node is identified as link faded node. FT structure invokes the RCM of that node to find its nearest optimal node for further communication. RCM consider only single hop nearest nodes.

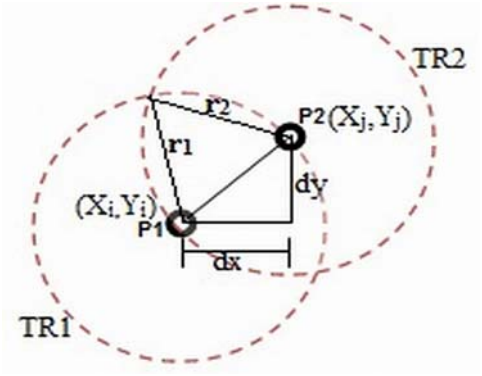

Fig. 5. Detecting mechanism of nearest node.

From Fig. 5, P_1 and P_2 are two node points located at X_i, Y_i and Xj, Yj with equal transmission range, *TR1* and *TR2* respectively. *dx* and *dy* are *X* and *Y* offsets of P_2 from P_1 (where [$dx = Xj - X_i$] and [$dy = Yj - Y_i$]

1) Determination of distance (*D*) of nearest node can be computed according to Pythagoras formula as

$$D = \sqrt{(dx \times dx + dy \times dy)} \quad (1)$$

If *D* from (1) is less then sum of the radii of the transmission range of two nodes, r_1+r_2, then the link faded node considers the new node as one of the solution to its replacement.

2) Before the random motion of the node 'n', the FT structure invokes the RCM of that node to find its nearest optimal node for further communication.
3) If the mobile node finds the nearest optimal node is a perfect alternative to replace its position, then its RCM send a Request notification (RN) to the new node.
4) If the new node accepts the request approach from the link faded node, it sends Acceptance notification (AN) by appending its own identities. The RCM of link faded node sends the NodeID of newly joined node to its upstream node (N_{n-1}) and then turns to inactive mode.
5) Now a new routing path is established. Then the newly joined node triggers its RCM and acquires the information set (IS_n). Thus, SF framework maintains the routing for the successful communication. Recovery of link failure mechanism is depicted in Fig. 6.

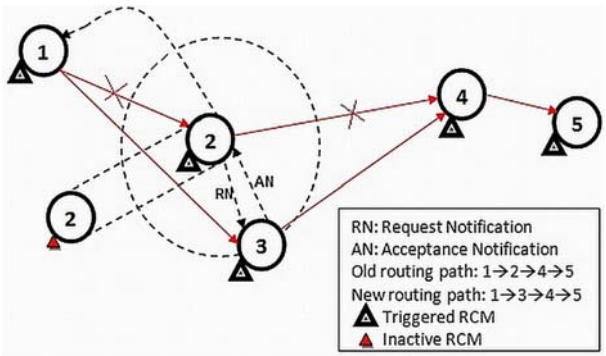

Fig. 6. Mechanism of RCM to evacuate link failure

We have implemented our SF Framework in Ad-Hoc network. We observed significant result. From the Fig. 7, we observed that the peak-pointed curves represent the occurrence of fault and deep swallow areas indicate the evacuation of faults during communication.

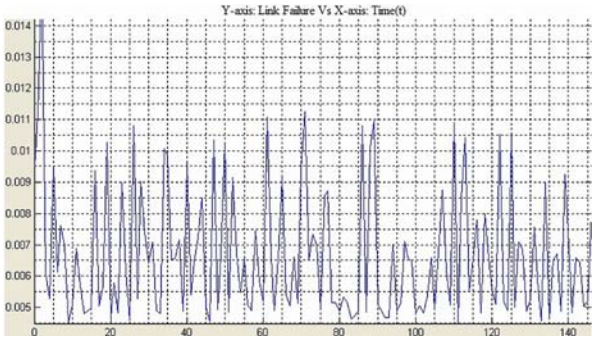

Fig. 7. Link failure Vs time (*t*)

3) Congestion identification and avoidance

After the establishment of routing path, the nodes that involve in the communication are blocked by RCM, to prevent the acceptance of new route establishment approach from new source node. Until the completion of communication, RCM holds the block. This blocking activity ensures the successful communication without the occurrence of congestion, between source node and target node. Fig. 8 depicts the contradiction relationship of QoD (Quality of Data) Vs Congestion rate during communication.

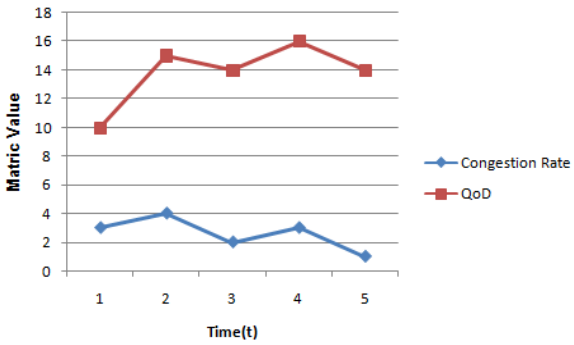

Fig. 8. Relationship between congestion rate and QoD.

Periodic checking of RCM enables the identification of node failure, link failure, and congestion failure and the corresponding fault is handled by fault evacuation management.

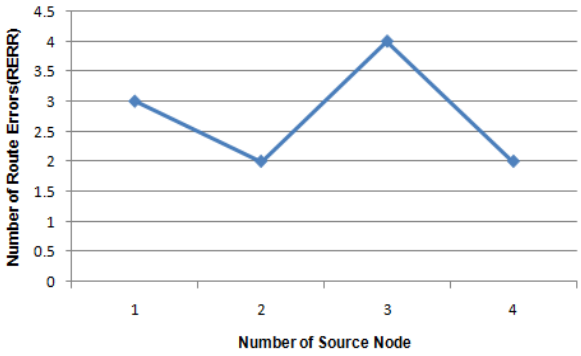

Fig. 9. Acquisition of RERR by Source node

Hence, from Fig. 9 we observed that the acquisition of Route Error (RERR) by source node is minimized by our SF Framework.

B. Impeccable Phase

This phase enables the network to be fault free based on the network change. The entire impeccable phase depends on the fault evacuation methods that are imposed by the FT structure of SF framework.

VI. Conclusion

Many Fault Tolerant solutions for Ad-Hoc networks have been proposed with diverse approaches. In this paper, after the establishment of routing path, our SF framework diagnoses the nature of faults and identifies the FT key requirements. Later, FT structure imposes its appropriate methods to eliminate the faulty effects. In our model we adopted DYMO for routing purpose. Our SF Framework improvises the optimal utilization of DYMO, by minimizing the acquisition of number of RERR by source node. Using our framework, we achieved the better efficiency by maintaining the optimal communication.

References

[1] T. Camp, J. Boleng, and V. Davies. "A survey of mobility models for ad hoc network research," Wireless Communications and Mobile Computing (WCMC): on *Mobile Ad Hoc Networking: Research, Trends and Applications*, vol. 2, no. 5, pp. 483–502, 2002

[2] I. D. Chakeres and C. E. Perkins, Dynamic MANET Ondemand routing protocol (DYMO). *Internet-Draft.* [Online]. Available: http://www.ietf.org/internetdrafts/Draft-ietf-manet-dymo-10.txt, July 2007.

[3] A. B. Malany and R. M. Chandrasekaran. "Mobility impact, timing analysis and repeatability issues of DYMO protocol in a precise mobile ad hoc network," *IJCSNS, International Journal of Computer Science and Network Security*, vol. 9, no. 6, June 2009

[4] A. Derhab and N. Badache, "Data replication protocols for mobile ad-hoc networks: a survey and taxonomy," Dept. of Computer. Eng., CERIST, Algiers. *Communications Surveys and Tutorials*, IEEE Issue Date: Second Quarter 2009, vol. 11, no. 2, pp. 33 – 51. ISSN: 1553-877X

[5] W. L. Li, D. Liu, and H. Zhao. "Fault-tolerance mechanism of mobile agent in mobile Ad-Hoc network," in *Proc. Wireless Communications, Networking and Mobile Computing*, 2008.

Karthick Raghunath is currently an Assistant Professor in the Department of Computer Science at Adhiyaman College Of Engineering, India. He received his B.Tech in Information Technology from Anna University, Chennai in 2008 and received his Master of Engineering in Pervasive Computing Technologies from Anna University of Technology, Tiruchirappalli in 2011. Since winter 2012, he has been pursuing his Ph.D. degree in the Department of Computer Science Engineering at Anna University of Technology. His research interests include Wireless sensor networks, Pervasive Computing and Nano Technology. Karthick is a member of IACSIT and IAENG.