ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Nailing Network Partition in Ad Hoc Network

S.Vijayalakshmi*
Research Scholar
IFET College of Engineering,
Villupuram, Anna University, Chennai, India
anviji_lakshmi@yahoo.co.in

S. Albert Rabara
Associate Professor
St. Joseph's College, Bharathidasan University
Trichy -2, India
a_rabara@yahoo.com

Abstract: In wireless ad-hoc networks, network partitioning occurs when the mobile nodes move with diverse patterns and cause the network to separate into completely disconnected portions. Network partitioning is a wide scale topology change that can cause sudden and severe disruptions to ongoing network routing and upper layer applications. Its occurrence can be attributed to various reasons like node getting overloaded, broken, selfish, malicious and hand off (Graceful and Abrupt leave) etc. The objective of this paper is to propose a mechanism by name Destitute Node Collaborative Cure Culminating to Continued Connectivity (DNC^5) and Network Partition Panic Packet (NP^3) which underpins the creation of two lists namely Core Routing List (CRL) and Backup Routing List (BRL) for any sender – receiver pair. The intermediate node causing network partition/divide under the influence of the attacker offers seamless interconnectivity through this innovative technique. This solution encourages the activation of BRL in absence of the CRL service to guarantee faultless/flawless network routing service in ad hoc network. The destitute nodes which are deprived of the network service due to network split unite/collaborate in desecrating the culprit node to cure the network split and render uninterrupted network activities. The proposed solution offer remote opportunities for the orchestration of network partition in ad hoc network. Suitable graphs have been simulated to accentuate the finding with judiciously considered parameters.

Keywords: Network Partition, Ad hoc Network, Core Routing List, Alternate Routing List and Network Partition Panic Packet

I. INTRODUCTION

Ad-hoc networks are temporary, decentralized, distributed self-organizing networks capable of forming a communication network without relying on any fixed infrastructure. The nodes of the network communicate each other over wireless channels. All nodes can function, if needed, as relay stations for data packets to be routed to their final destination. In other words, adhoc networks allow for multi-hop transmission of data between nodes outside the direct radio reach of each other. MANETs have been widely used for tactical military communication systems. The United States Defense Advanced Research Project Agency (DARPA) has sponsored projects such as the Near-Term Digital Radio (NTDR) system to control infantry, armor, and artillery units in battle field scenarios where no communication infrastructure exists [1].

The study of network topology plays an important role in designing routing protocols. The failure of set of links or nodes in the underlying network can cause the network to break away into two or more components or Clusters. As a result of this, nodes within a cluster can communicate each other, but there is no communication across the nodes in different cluster. This phenomenon is called network partitioning, visualized as graph partitioning. Needless to say mobility of nodes is the main cause for the network partition. Very often the network will partition and remerge. Due to this, nodes from the different clusters try to route the packets without success and hence tries to explore new routes, which will be unsuccessful. These result in lot of route requests and route reply packets triggered from the nodes, which ultimately bring down the performance of the network due to congestion [2]. Besides, network partition causes a serious consequence in the performance of adhoc networks which encourages distributed and client server applications. In this kind of applications, specified task is distributed among the nodes of the network and they exchange the information in order to complete it. But on the occurrence of partition, they fail to do the intended operations, which require data from other cluster [3].

Providing security support for mobile ad-hoc networks is challenging for several reasons: (a) wireless networks are susceptible to attacks ranging from passive eavesdropping to active interfering, occasional break-ins by adversaries (b) mobile users demand "anywhere, anytime" services; (c) a scalable solution is needed for a large-scale mobile network (d) Dynamic topology (e) infrastructure less (f) Peer –to-peer network (g) Lack of centralized authority. Examples of applications for ad hoc networks range from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture [4]. This challenge intense environment when coupled with network partition unfolds many intricacies to the smooth conduct of routing in ad hoc network.

A. *Reading Roadmap*

This paper starts with this section, which gives a brief introduction of this paper. **Section 2** presents the network partition in ad hoc network. The proposed model is presented in **Section 3**. Simulation study is expounded in **Section 4. Section 5** elucidates the related work. Finally conclusions are given in **Section 6**.

II. NETWORK PARTITION IN ADHOC NETWORK

In wireless ad-hoc networks, network partitioning occurs when the mobile nodes move with diverse patterns and cause the network to separate into completely disconnected portions. Routing in ad hoc network is a complex process as each node act as a self made router. The participating node computes/establishes the route on their own to the destination with the support and service extended by the intermediate nodes. The intermediate nodes clearly emerge as a route service provider (RSP) and underpin the inevitable cooperative and collaborative behaviour existing in the network [5]. This accentuates the fact that the routing in adhoc network is influenced by the behaviour and performance of the intermediate nodes to a greater extent. The expected functionality and role of the intermediate nodes is not always in accordance/compliance with the prior defined security policies for the smooth conduct of routing in ad hoc network. The misbehavior of the intermediate node can be attributed to either of the following reasons like Frequent Node Movement (Dynamic Topology), Selfish, Overloaded, broken and Malign nature [6]. The malicious intent of the IN is to cut off the services to the nodes which lead to the formation of new isolated and unreachable cluster. The malfunctioning of the already created route or the one to be created is influenced by other cited problems only if the situation warrants. The perpetuation of malicious behavior exhibited by IN is wrought by a range of attacks like DoS, Blackmail, Sybil, Hello Flood and Rushing attack.

Network Partition is an attack where the spurious intermediate nodes forward fabricated/mismanaged report about its neighbors and cause the network division. The ulterior motive is to prune the genuine nodes from the network vicinity and deprive it from receiving/delivering the network services to its neighbor. It is important at what stage the partition is detected: whether it is before (predetection) or after it happens (post-detection.) If the partition is predicted before it happens, then routing algorithms can adopt to reduce the congestion, which is the aftereffect of the partition [7]. These algorithms are devised at the cost of more processing and computation which reduces the performance of the network and also power constraints arise. In the post detection approach, the partition is detected immediately after it occurs. These methods do not over utilize the scarce resources, but due to network partition, till it is detected the performance of the routing protocols and network throughput reduces due to congestion. Hence there should be a trade off in selecting and devising both the methods to detect network partition [8].

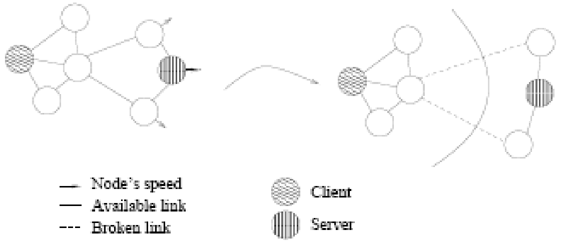

Figure 1: Network Partition Caused by Topology Changes.

III. OVERVIEW OF THE PROPOSED SYSTEM

This paper advocates the concept that a node in ad hoc network is holding two routing list namely CRL (Core Routing List) and Alternate/Backup Routing List (BRL). The CRL nodes are the primary source of routing information which gets updated and exchanged between the intermediate nodes to construct a valid route leading to destination. The inclusion and exclusion of the CRL intermediate nodes is automatically adjusted to accommodate the dynamic topology nature of the ad hoc network. The selection of CRL nodes is a stringent process that presses the participating nodes to qualify various tests posed by the genuine sender and other intermediate nodes. The possession of optimal values for potential parameters like CONFIRM ROUTE REQUEST (CRREQ), CONFIRM ROUTE REPLY (CRREP), FURTHER ROUTE REQUEST (FRREQ), FURTHER ROUTE REPLY (FRREP) etc elevates the node to be a part of CRL. The ad hoc network requires the service of BRL in case of CRL encountering an irrecoverable failure. The node equipped with both lists ensures resilience to various attacks by invoking the alternate route when the prime route fails. The network partition in network can stem from either malicious reasons or due to unpredictable network topology configuration. The mechanism which we have proposed is a pro active measure which endorses the idea of creation of two lists to curtail the incidence of network partition that surface due to the wrong reasons. The routing algorithms of BRL nodes are accordingly adjusted to defend the network from the clutches of the adversaries causing network division.

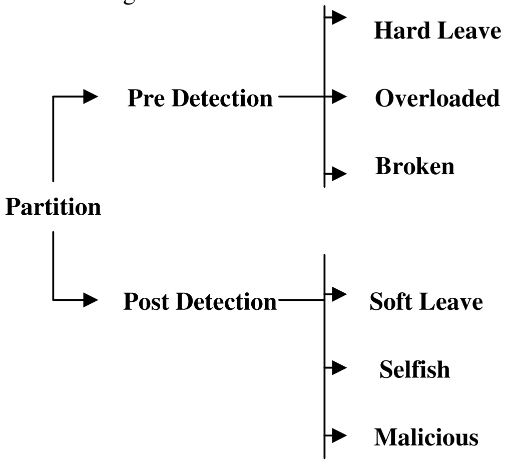

Figure 2: Analysis of Network Partition.

The nodes in ad hoc network may experience frequent hand off due to the mobility nature. The spurious nodes unlike the genuine nodes abruptly drift from the network in an impromptu fashion causing a wide level network split and leave less time for the network to recover and heel from the disaster. The departing node informs well in advance to its neighbors and gives enough time and support to reestablish the to-be distorted network path. This graceful leave by the node minimizes the alternate route creation overhead and latency and boost the network performance. The non receipt of data (both control and session) by the CRL node for a considerable period of time from its neighbor creates room for suspicion. The doubting/troubled CRL node seeks the service from the BRL nodes to target the culprit node that is playing a spoil sport. The node that is deprived from the normal routing service is labeled as Destitute/Deprived Node (DN). The DN in CRL unitedly joins hands in cornering the spurious adversary that has caused a network split. This network gesture incites the information exchange between the DN and its immediate neighbor or to the sender to trigger remedial measure thereby ensuring the continued connection. Various clusters of differing capacity and architecture emerge as an offshoot of network partition. Destitute Node from multiple clusters also can handshake with each other and target the adversary by flooding the Network Partition Panic Packet (NP^3) to the sender. This novel mechanism by name Destitute Node Collaborative Cure Culminating To Continued Connectivity (DNC^5) helps the destitute node that are divested from the network routing services to ensure uninterrupted and unprecedented network association and relation. The possibility that the BRL nodes also falling prey to attackers is high. The failure of BRL nodes in the routing process is addressed by promoting the BRL'S BRL (secondary) as CRL to ensure seamless connectivity amidst the presence of unscrupulous nodes causing network split.

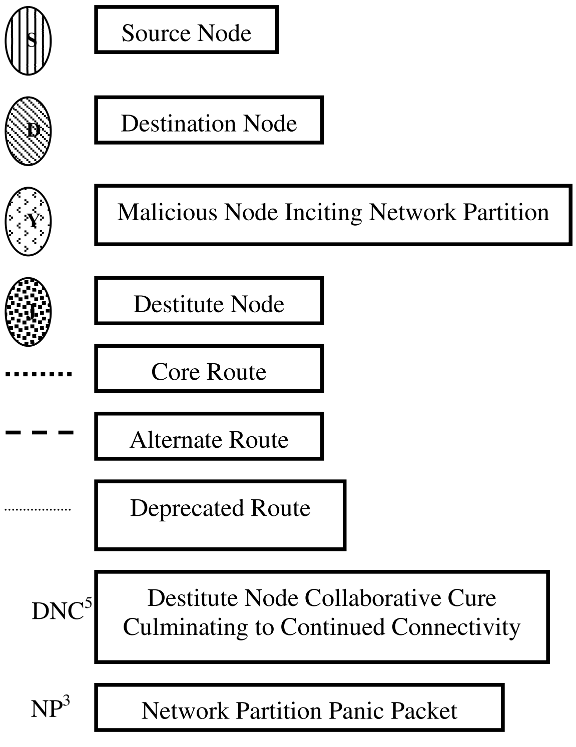
S
Source Node
D
Destination Node
Y
Malicious Node Inciting Network Partition
I
Destitute Node
Core Route
Alternate Route
Deprecated Route
DNC^5
Destitute Node Collaborative Cure Culminating to Continued Connectivity
NP^3
Network Partition Panic Packet

Figure 3: Notations Used in Network

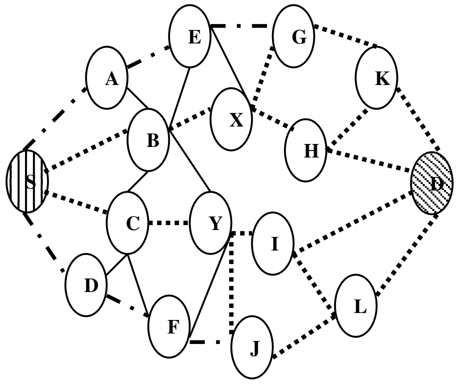

Figure4: Ad hoc Network with BRL and CRL

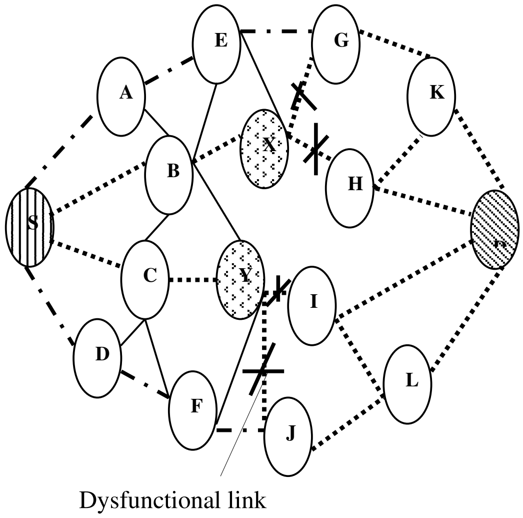

Figure 5: Ad hoc Network Exhibiting Dysfunctional Link

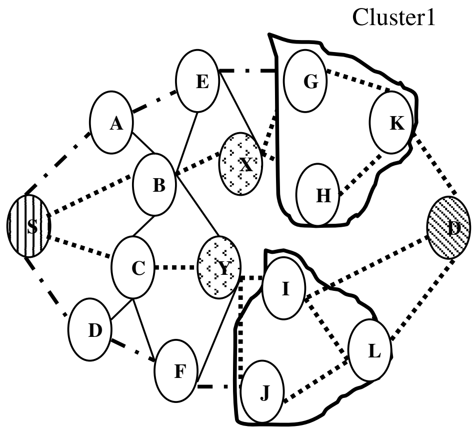

Figure 6: Dysfunctional Link Leading to Disjoint Clusters

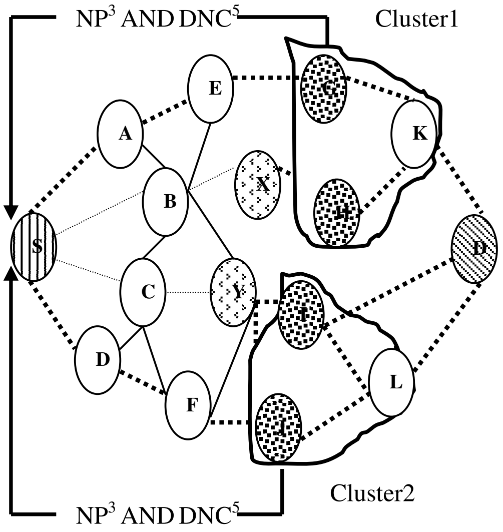

Figure 7: Deprived Nodes Prosecuting the Culprit using two Novel solutions like NP^3 and DNC^5

IV. SIMULATION STUDY

The simulation study and associated graphs attest to the fact the larger the number of misbehaving nodes in ad hoc network the higher the degree of network partition. The origin of Network partition stems from various factors like overloaded, selfish, broken and malicious nature. The network partition occurring due to the former reasons can be anticipated in advance and proactive remedial measures can be prescribed for enabling the recovery from the clutches of network partition. The latter unanticipated reason/trait thoroughly mars the normal routing in ad hoc network which underpin the need for adoption of stringent security solution for arresting the occurrence of the network partition/split [9]. The idea proposed in this paper propounds the creation of two lists namely CRL and BRL to offset the mismanagement of the intermediate nodes causing network split. A graph has been simulated to study the impact of network split on the mean latency metric. Mean Latency is defined as the average time elapsed from when a data packet is first sent to when it is first received at its destination. The number of misbehaving intermediate node is taken along the X axis and the Mean Latency metric is taken along y axis. The effect of the proposed solution is validated by constantly monitoring the mean latency metric in the presence and absence of the recommended solution. It is learnt from the graph that the mean latency of the packets is continuously maintaining a consistent trend despite the network partition in the presence of the suggested solution. The non adoption of the solution mechanism gradually pulls down the mean latency metric as the sent packets are deflected away from the normal routing path.

V. RELATED WORK

Rajan, A.M et al. [1] proposed a new characterization of group mobility based on existing group mobility models, which provides parameters that are sufficient for network partition prediction. We then demonstrate how partition prediction can be made using the mobility model parameters, and illustrate the applicability of the prediction information. They demonstrate how partition prediction can be made using the mobility model parameters, and illustrate the applicability of the prediction information

Michael Hauspie et al. [2] proposed an original link robustness evaluation method based on the notion of disjoint paths set that allow efficient partition detection without using any kind of positioning system. After showing that the use of disjoint path is relevant for detecting network partitions, we propose a distributed algorithm that collects disjoint paths available between the server and the client and
thus show that our partition detection metric can be used in a real network.

Park et al. [3] proposed TORA, an adaptive routing protocol for ad-hoc networks. In this protocol, the authors use a method to detect network partitions after they occur. The aim of this detection for their routing algorithm is to find the nodes that are no more reachable and thus, erase the deprecated routes that lead to them. In this paper, we do not focus on detecting partition after its occurrence but before, so that applications can react by modifying their behavior while the nodes are still connected. Detecting network partition before they happen give some time to seamlessly react by finding a new route and/or adapt the application behavior.

Shah *et al.* [4] aimed at enhancing data access in an ad-hoc network by detecting partitions before it happens. In their scenario, a node n1, needs data that are stored in another node (say node n). For allowing n1 to access the data even if its connection with n2 physically breaks, they propose a data replication mechanism based on partition detection. Every node embeds a positioning system (such as GPS) and by successive measures computes its velocity. Regularly, it spreads those information to the other nodes. Thus, each node of a connected group knows the behavior of the other members of this group. So, they can *predict* when a node storing a particular data will leave the group before it effectively does it. At this point, the owner of the data elects a node of the group to be another host of the data and replicates it on this node. The main advantage of this method is that each node knows exactly *when* the partition occurs if node movements are almost regular (no brutal direction changes).

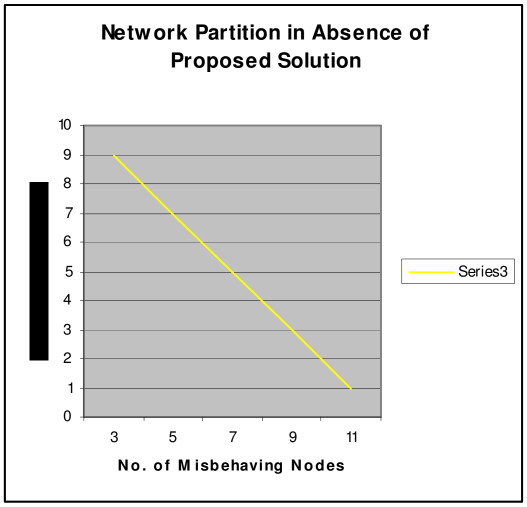

Figure 8: Network Partition in Absence of proposed solution

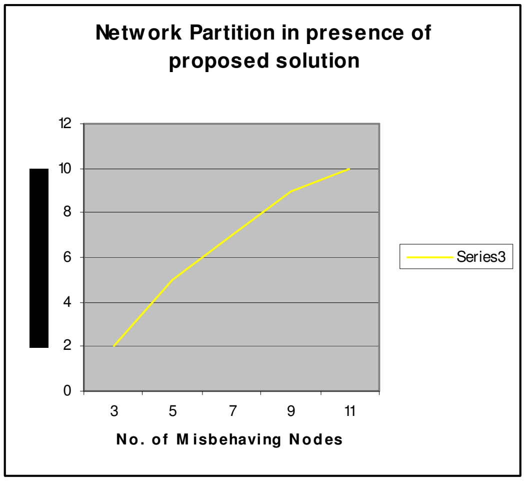

Figure 9: Network Partition in Presence of proposed solution

VI. SUMMARY AND FUTURE WORK

The ad hoc network is confronted with an array of attacks of which network partition assume a special importance. This attack perpetrates by splitting the network in to numerous disjoint clusters devoid of contact/connectivity between them. The solution proposed is to deploy two routing lists namely Core Routing List CRL and Backup Routing List BRL to ensure continued connectivity by activating a technique by name Destitute Node Collaborative Cure Culminating to Continued Connectivity DNC[5.] This novel and innovative technique offers full resistance from the influence of the nodes causing network partition. The efficiency of the proposed solution is evaluated using Network Simulator tool by drawing graph containing No. of misbehaving middle nodes in X axis and the Mean latency metric in Y axis. The network partition caused by collective node labeled as aggregate split becomes the foreseeable enhancement.

VII. REFERENCES

[1] RAJAN, A.M., Chandra, M.G., Reddy, L.C. And Hiremath, P., “A Study On Network Partition Detection Relevant To Ad-Hoc Networks: Connectivity Index Approach” In The IJCSNS International Journal Of Computer Science And Network Security, VOL.8 No.6, June 2008.

[2] Hauspie, M., Carle, J., Simplot, D., “Partition Detection In Mobile Ad Hoc Networks Using Multiple Disjoints Paths Set”.

[3] V.D.Park And M. Scott Corson, A Highly Adaptive Distributed Routing Algorithm For Mobile Wireless Networks, In Proceedings Of IEEE INFOCOM ’97, Kobe, Japan, April 1997.

[4] Shah, S.H, Chen, K. And Nahrstedi, K., Cross-Layer Design For Data Accessibility In Mobile Ad Hoc Networks, In Proc. Of 5th World Multiconference On Systemics, Cybernetics And Informatics (SCI 2001), Orlando, Florida, July 2001.

[5] Y.C. Hu, A. Perrig, D.B. Johnson, Ariadne: A Secure Ondemand Routing Protocol For Ad Hoc Networks, In: Proceedings Of ACM Mobicom 2002, Atlanta, Georgia, September 2002.

[6] Nguyen, H.L. And Nguyen, U.T., “A Study On Different Types Of Attacks On Multicast In Mobile Ad Hoc Network”, Adhoc Networks 6(2008) Pages 32-46.

[7] R. Curtmola And C. Nita-Rotaru, “BSMR: Byzantine-Resilient Secure Multicast Routing In Multihop Wireless Networks”, Ieee Transactions On Mobile Computing, Vol. 8, No. 4, April 2009.

[8] R. Chandra, V. Ramasubramanian, And K. Birman, “Anonymous Gossip: Improving Multicast Reliability In Mobile Ad-Hoc Networks,”Proc. 21st Int’l Conf. Distributed Computing Systems (ICDCS ’01), 2001.

[9] Y.C. Hu, A. Perrig, D.B. Johnson, Rushing Attacks And Defense In Wireless Ad Hoc Network Routing Protocols, In: Proceedings Of ACM Wise 2003, San Diego, CA, September 2003.