IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VI (Feb. 2014), PP 06-10
www.iosrjournals.org

Design and Developing a Multicast Routing Protocol for Link Failure and Reliable Data Delivery.

M. Selvi[1], Dr. R. Balakrishna[2]
[1]*Asst. Professor, Dept of CSE, A.C.S Engineering College, & Research Scholar, Dept of CSE, RRCE, Bangalore-74*
[2]*Professor & Head, Dept of ISE, RajaRajeswari College of Engineering Bangalore,560074, India*

Abstract: *MANET is a mobile Ad hoc network. It is a wireless and self organized network without infrastructure support. Ad hoc networks systems possess rapid deployment, robustness and flexibility. The problems of Ad hoc network share dynamic network topology and structure. That is, nodes may join or leave the network, causes link failure in the network and also the limitation of radio range defined by transmission power communicating parties are not within the transmission range. Movement of the intermediate node result is path failure. Otherwise links in the networks may share resources such as conducts or ducts and the failure of such shared resources results in failure of multiple links. To avoid the link failure, multicasting protocol (NAMP) will be used in the research. NAMP could overcome the observed problem and improve the performance of data delivery. Special protocol called security protocol for reliable data delivery (SPREAD) is also used in the research.*

Keywords: - *NAMP, SPREAD, LINK FAILURE, DATA DELIVERY.*

I. Introduction:-

A mobile ad hoc network (MANET) is a self-configurable, self-organizing, infrastructure less multi-hop mobile wireless network. By self-configurable and self organizing, we mean that a MANET can be formed, merged together, or partitioned into separate networks on the fly, depending on networking needs; and few administrative actions need to be performed for network setup and maintenance. By infrastructure less, we mean that a MANET can be promptly deployed without relying on any existing infrastructure (such as base stations for wireless cellular networks). By multi-hop wireless, we mean that in a MANET, the routes between end users may consist of multiple wireless hops, as compared to the single wireless hop in a wireless local area network (WLAN) or a cellular network, where only the last hop (e.g., from the end user to the access point or the base station) is wireless; and all the links beyond that point remain wired. In addition, each node in an ad hoc network is capable of moving independently; thus the network topology can change continuously and dramatically.

Each node also functions as a router that discovers and maintains routes to other nodes and forwards packets for other nodes. Rapidly deployable and self-organizing features make the ad hoc network very attractive in tactical and military applications, where fixed infrastructures are not available or reliable; and fast network establishment and self reconfiguration are required. Primary applications of an ad hoc network include tactical communication in a battlefield, disaster rescue after an earthquake.

Five major security goals that need to be addressed to maintain a reliable and secure Ad hoc Environment are as follows:

1. Confidentiality
2. .Availability
3. .Authentication
4. . Integrity
5. Non – repudiation.

Routing protocols are classified into three categories:

a) **Proactive: -** It continuously learns the topology of the network by exchanging information among the network nodes. Whenever there is need for a route from source to destination, such route information is available immediately. If the network topology changes frequently, the cost of maintaining the network might to be very high. If the network activity is low, the information above actual topology might not be used.
b) **Reactive: -** It query reply dialog and establishes routes only when the need arises.
c) **Hybrid: -**Often reactive or proactive features of a particular routing protocol.

Based on data delivery classification of MANET routing protocols are uni-cast and multicast.

Uni-cast: - Send data from single source to single destination.

Multicast: - Is the delivery of information to a group destination simultaneously using the most efficient strategy to deliver the messages over each link of the network.

Create copies only once when the links to the destination split. Multicast routing protocol for MANET uses both multicast and uni-cast for data transmission. Multicast again divided into two categories

1. **Tree based:-** Maintain only one path
2. **Mesh based:-** Maintain several path

Problem Identification: - Security is a critical issue in a mobile Ad hoc network (MANET) .Therefore I propose NAMP and SPREAD to improve robustness as well as reliable data delivery in the Ad hoc network.

II. Literature Survey:-

1. Alsakib, Pathon, Muhammad Monowar, Muhammad Alam, Choonghung "Neighbor aware multicast routing protocol for mobile Ad hoc network". The international Arab Journals of information technology vol.5, No.1. Jan. 2008. In mobile Ad hoc network many protocols were introduced, but only familiarly protocols like TCP, UDP, and AODV are only worked by users. So in the year 2008, NAMP was introduced. The existing system of this protocol was dominant pruning flooding method but performance was found to be less in delivery of packet. Therefore trusted dominant pruning flooding method is proposed in the research to avoid misbehaving node becoming a member of the conducted dominant set and combined with security protocol for reliable data delivery to overcome the existing problem.
2. Kayi Lee Hyang-Won Lee and Eytan Modiano "Reliability in Layered Networks with Random Link Failures".This work was supported by NSF grants CNS-0626781 and CNS-0830961 and by DTRA grants HDTRA 1-07-1-0004 and HDTRA-09-1-005. Generally the network reliability is considered. The setting of logical link failure can be co related even if physical link fail independently. So avoid this, light path algorithm was suggested in this paper. The purpose is approximately the failure polynomial by estimating the values of its co efficient. However Tree based hybrid protocol is proposed in the research instead of any algorithm to recover the link failure. It utilizes the neighborhood information. The roots in the network maintained by networks and reply messages. This concept is referred has a neighbor aware multicast routing protocol.
3. HamzaAldabbas, Tariq Alwada'n , HelgeJanicke, Ali Al – Bay Atti "Data Confidentiality in Mobile Ad hoc Network". International journal of wireless and mobile network (IIJWMN) Vol.4, No.1, Feb. 2012. It was observed in this paper that transfer the data securely by using the policy mechanism, that is policy enforcement point in and out, policy decision point and controller. Based on this, the simulation configured the send and receives function to achieve the functionality of this component policy. Decision point is used to share source code to achieve the functionality of component in all nodes. Controller is used to store the information, receive from the other components. It is proposed in the research to use security protocol for reliable data delivery for secrete sharing between nodes and overcome the problem for colluded attacks and this is high network performance.

Objectives:-

Recovering the link failure and reliable data delivery are the most important research problem in the networking system. This problem is avoided normally by using architecture. This may be to increase many types of architecture for similar problem. To recover the link failure and reliable data delivery based on NAMP and SPREAD.

The basic features of NAMP and SPREAD is lower latency, storing topology information is more efficient, reduce bandwidth utilization for mass distribution of data and the basic idea is to transform a secret message into multiple shares by secret sharing scheme; and the deliver the shares via multiple paths to the destination, so that even if a small number of the nodes used to relay messages are eavesdropped, the secret message as a whole is not eavesdropped.

III. Methodology:-

1. NAMP 2.SPREAD

NAMP: - Neighbor – Aware Multicast Routing Protocol (NAMP). This is a tree based hybrid routing protocol utilize neighborhood information to route in the network maintained by request and reply message. If the receiver is not within the range, it searches the receiver by using dominant pruning flooding method. NAMP consist of the tree structure i) Multicast Tree Creation ii) Multicast Tree Maintenance iii) Joining and Leaving of nodes from the multicast group. To create a multicast tree source, node sends a flood request packet to the destination with data payload. During the process of forwarding the packets, each node selects a forwarder and creates a secondary forwarder list (SFL). It contains the information about the nodes that were primarily considered as possible forwarders. Each intermediate node that use the chosen forwarder to forward the packet, but keeps the knowledge about other possible forwarders in SFL. SFL issued for repairing any broken route in the network. Link failure recovery is one of the greatest advantages of NAMP.

Fig:1General Network

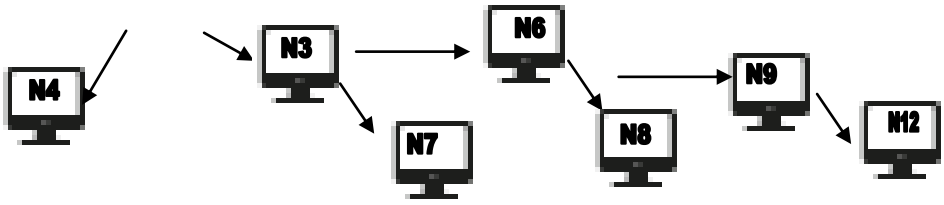


Fig: 2Link Failure Network

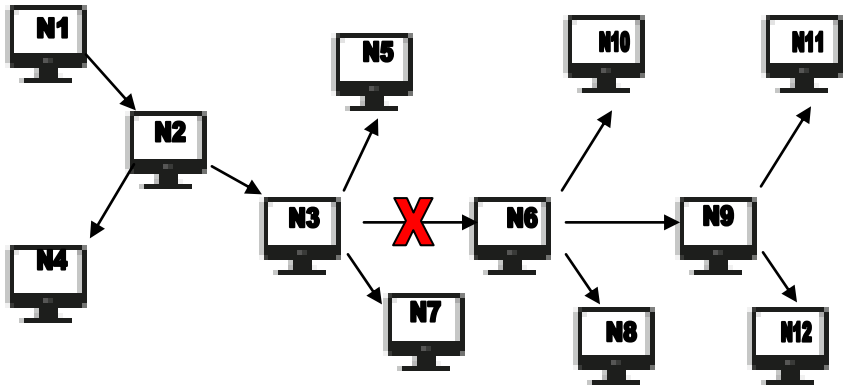
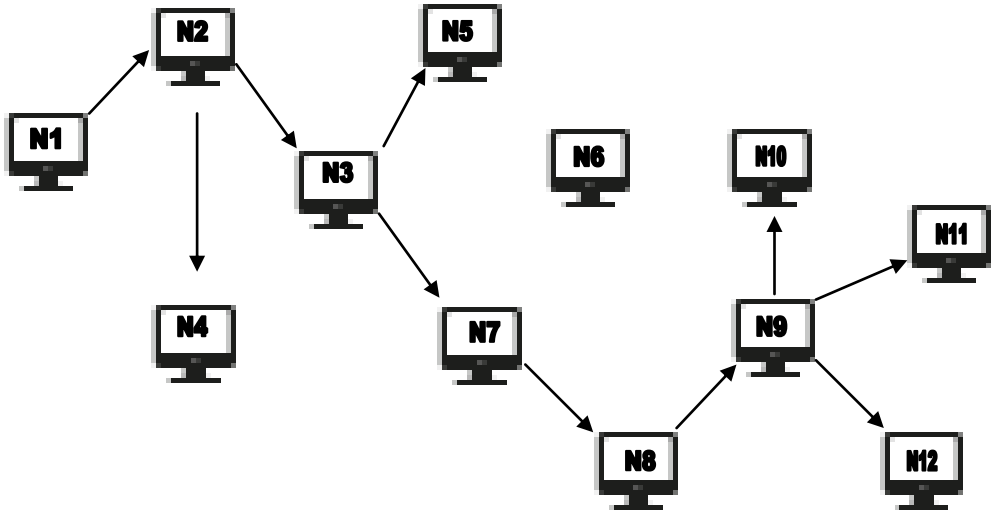
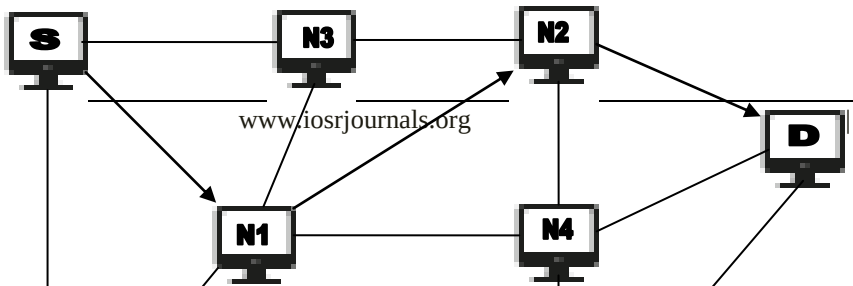


Fig: 3Recover Link Failure Network



SPREAD: - Security Protocol for reliable data delivery (SPREAD) is a hybrid protocol. It provides data confidentiality security service in routing protocol. It uses secret sharing scheme between neighboring nodes to strengthen data confidentiality. It overcomes a problem of eaves dropping and colluded attacks. It's essential requirement is threshold secret sharing. Designing efficient routing protocol that provides both high security and high network performance.

Fig:4Find The Most Secure Path In The Transformed Graph



Fig;5 Edge Regrouping

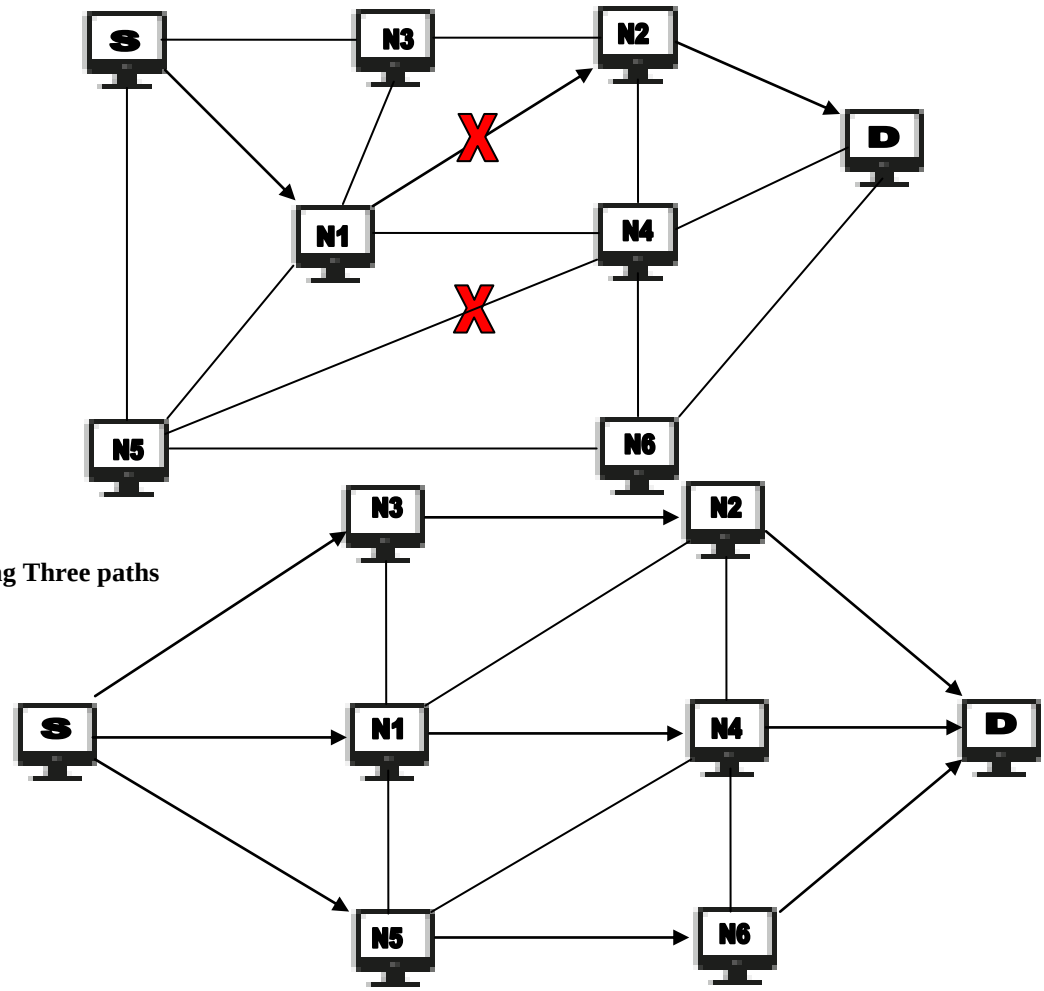


Fig:6 Resulting Three paths

Possible Outcome: - The possible result of NAMP and SPREAD is improve the performance of the network by taking less time to transfer packets from the source to the destination(s) and more secure also provides a certain degree of reliability because of the redundancy introduced without compromising the security.

Acknowledgements: The author's wishes to express thanks to the management of Rajarajeswari Group of Institutions, Bangalore, Principal ACS and RRCE Bangalore for their support and encouragement during this research studies.

References: -

[1]. AleksiPenttinen," Research Ad hoc network: current activity and future direction",NetworkingLaboratory,Helinski University of Technology,FIN-02015 Hut,Finland 2002.

[2]. ImrichChlamtac[a],MarcoConti[b],Jennifer J-N.Liu[c]," Mobile Ad hoc network imperatives and challenges",www.elsevier.com/locate/adhoc networks.2003 13-64.

[3]. Umang Singh" Secure routing protocol in mobile Ad hoc network - a survey and taxanomy".International Journal of reviews in Computing Sep 2011 Vol:7 IJRIC and LLS E-ISSN 2076-3336.

[4]. C.Sreedhar,Dr.S.MadhusudhanaVerma,Prof.N.Kasiriswanath" A survey an security issues in wireless Ad hoc network routing protocol"in IJCSE International Journal on Computer Science and Engineering vol 2,No.02,2010,224-232.

[5]. TanuPreetSingh,ShiraniDua,VikrantDas"Energy Efficient Routing Protocols in Mobile Ad hoc Networks",in IJAR CSSE International journal of Advanced research in Computer science and Software Engineering vol 2,Issue 1,January 2012 ISSN:2277 128X

[6]. G.VijayaKumar,Y.VasudevaReddy,Dr.M.Nagendra" Current research work on routing protocol for MANET: a Literature survey"IJCSE IJCSE International Journal on Computer Science and Engineering vol 2,No.03,2010,706-713.

[7]. Sunil Taneja and AshwaniKush"A Survey of Routing Protocols in Mobile AdhocNetworks".International Journal Of Innovation ,Management and Technology,vol 1,No.3,August 2010,ISSn 2010-0248.

[8]. Arun Kumar Bayga,SiddharthaGupte,Yogesh Kumar Shukla,AnilGaikapati" Security in Ad hoc networks"CS685 Computer Science Department University of Kentucky.

[9]. FranckLegendra,TheusHossmann,FelixSuttan,BernhardPlattner" 30 Years of wireless Ad hoc network research: what about humanties and disaster relief solution what are we still missing? ACWR'11 Dec 2011.

[10]. HamzaAldabbag,TariqAlwada'nHelgeJanicke,AliAl.Bayatti"Data Confidentiality in Mobile AdhocNetworks"International Journal of Wireless and Mobile Networks(IJWMN) vol 4,No.1 February 2012.

[11]. Wenjinglou"SPREAD:Secure Protocol for Reliable Data Delivery"Thesis of Doctors of Philosophy,University of Florida,2003.

[12]. Al-Sakibpathan,MuhammadMonowar,Md.Rabbi ,Muhammad Alam and ChoongHong."NAMPNeighbor – Aware Multicast Routing Protocol for Mobile Ad hoc Networks".The International Arab journal of Information Technology Vol 5,No.1,January 2008.

[13]. Kayi Lee, Hyang-won Lee and EytanModiano" Reliability in layered networks with random link failures" Massachusetts Institute of Technology Cambridge, this work was supported by NSF grants CNS-0626781 and CNS-0830961 and by DTRA grants HDTRA1-07-0004 and HDTRA-09-1-005

[14]. AshikurRahman,RawelGburzynski,BozenaKaminska "Enhanced dominant pruning based broadcasting in untrusted Ad hoc network",at the direction of IEEE Communication Society Subject Matter Expersts for Publication in the ICC 2007 Proceedings.

[15]. Gang Xu,eristianBrucea,LiviuIftode"A policy Mechanism for Trusted AdhocNetworks"at IEEE Transactions on Dependable and Secure Computing VOl.8,No.3 May –June 2011.

[16]. pathan A-sk,AlamMM,MonowarMM,Rabbi MF(2004)"An Efficient Routing Protocol for Mobile Ad hoc Network with neighbor Awareness and Mulitcasting Proceedings of IEEE E-Tech,july 2004 97-100.

[17]. Lim H,Kim C (2000) Multicast tree Construction and Flooding in Wireless Ad hoc Networks,Proceedings of the 3rdACm International Workshop on Modeling,Analysis and SSimulation Of Wireless and mobile Systems 61-68.

Authors Biography

Selvi M, Asst.Professor, Dept of Computer science and engineering, ACS college of engineering , Bangalore. She has completed her M.Tech in computer science and engineering at --- Dr.M.G.R.University. Her research interest are in the field of Mobile Adhoc Network, Network Security, Theory Of Computation ,Compiler Design , Computer Networks. She has published over 07 National and International Conferences various papers across India. She is the Life member of Indian Society for Technical Education. Presently .Registered Ph.D under visveraya Technological University.

Dr. R.Balakrishna, Professor and Head, Dept of Information Science and Engineering, Rajarajeswari College of Engineering, Bangalore. He has completged his Ph.D in Computer Science and Technology at Sri Krishnadevaraya University, Anantapur,AP. M.Tech in Computer Network Engineering at Maharshi Dayanad University. His research interests are in the field of Wireless ad hoc network, Sensor network, Artificial Neural Networks, Data mining, Operating System and Security. He has published over 28 International Journals , 26 National & International Conferences various papers across India and other countries. He is the Life member of Indian Society for Technical Education, IAENG, CSI.