International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

NOVEL ROUTING STRATEGY IN DISTRIBUTED WIRELESS NETWORKS

Sayikrishnan.H
RVS College of Engineering and TechnologyCoimbatore
skris18@gmail.com

MR. P.CHANDRASEKAR. M.E
Assistant Professor
RVS College of Engineering and Technology
Coimbatore

Abstract—Energy awareness for protocol management is becoming a crucial factor in the design of protocols and algorithms. On the other hand, in order to support node mobility scalable routing strategies have been designed and these protocol try to consider the path duration is more as consider .For better path duration and link stability this paper proposed the performance based on LAER AND GPSR and evaluate based on some parameters and clusters is added in proposed methodology for avoiding large path transmission.

Index Terms—MANET, scalable routing, link stability, energy consumption, clusters

INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can be inter networked in areas without a preexisting communication infrastructure radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network.

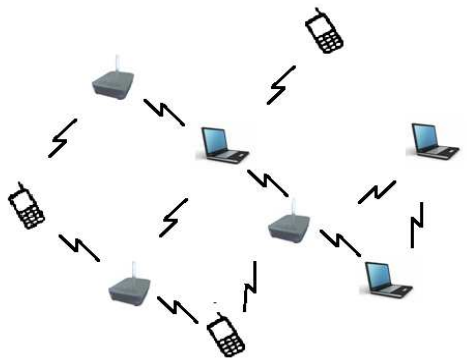


Figure 1.1 Manet

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

1.2. Vulnerabilities of the Mobile Ad Hoc Networks

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, discuss the various vulnerabilities that exist in the mobile ad hoc networks

1.2.1. Lack of Secure Boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundaryin the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. In the wired network, adversaries must get physical access to the network medium, or even pass

through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network.

1.2.2. Threats from Compromised nodes Inside the Network

There is no clear secure boundary in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network. Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

1.2.3. Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner. First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a convincing conclusion that the failure is caused by an adversary. However, can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that can safely conclude that all of the failures caused by this adversary should be malicious failure instead of benign failure, though these failures occur in different nodes at different time. From this example find that lack of centralized management machinery will cause severe problems when try to detect the attacks in the ad hoc network. Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network . In mobile ad hoc network, all the nodes are required to cooperate in the network.

1.2.4. Restricted Power Supply

Due to the mobility of nodes in the ad hoc network, it is common that the Nodes in the ad hoc network will reply on battery as their power supply method. While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. The first problem that may be caused by the restricted power supply is denial-of-service attacks. Since the adversary knows that the target node is battery-restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and the target node will be out of service to all the benign service requests since it has run out of power. Furthermore, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to cooperate with other nodes to support some functions in the network. Just take the cluster-based intrusion detection technique as an example. There

may be some nodes that behave selfishly and do not want to cooperate in the monitoring node election process, which will make the election fail if there are too many selfish nodes. Moreover, should not view all of the selfish nodes as malicious nodes: some nodes may encounter restricted power supply problem and behave in a selfish manner, which can be tolerated; however, there can be some other node who intentionally announces that it runs out of battery power and therefore do not want to cooperate with other nodes in some cooperative operation.

1.2.5. Scalability

Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

1.3. Security Solutions to the Mobile Ad Hoc Networks

Vulnerabilities that potentially make the mobile Ad HOC networks insecure However, it is far from our ultimate goal to secure the mobile ad hoc network if merely know the existing vulnerabilities in it. As a result, need to find some security solutions to the mobile ad hoc network.

1.3.1. Security Criteria

Before survey the solutions that can help secure the mobile ad hoc network, think it necessary to find out how can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network.

1.3.1.1. Availability

The term Availabilitymeans that a node should maintain its ability to provide all the designed services regardless of the security state of it . This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service .

1.3.1.2. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can becompromised mainly in two ways :

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

1.3.1.3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, need to keep them secret from all entities that do not have the privilege to access them.

1.3.1.4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

1.3.1.5. No repudiation

No repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

1.3.1.6. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, need to ensure that network management function is only

accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

1.3.1.7. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

1.3.2. Attack Types in Mobile Ad Hoc Networks

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types:

I. External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

II. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

1.3.2.1. Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power.

Impersonation attack is a severe threat to the security of mobile ad hoc network. As can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

1.3.2.3. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

II RELATED WORKS

C. Taddia, A. Giovanardi, G. Mazzini, M. Zorzi(PUBLISHED IEEE 2005).The paper compares the performance of the AODV, DSR[7],OLSR[28] classic routing protocols for ad hoc networks, when an IEEE 802.11b[2] MAC protocol is used. The investigation, performed by means of simulations, evaluates the energy efficiency of these protocols and the effect of the802.11b rate adaptation capability on the performance.

Qing Zhao, Member, IEEE, and Lang Tong, Fellow, IEEE(may 2005**).** An analytical approach to the characterization of energy consumption [4] of large-scale wireless networks is presented. The radio model includes energy consumption of nodes at various operating states. Analyze the total energy consumption[4] of the proactive and the reactive networking[6] strategies taking into account transmitting,. Scaling laws with respect to the increase of node density and geographical size are derived.

P. Bergamo, D. Maniezzo, A. Travasoni, A.Giovanardi, G.Mazzini,M.Zorzi (IEEE2003**).**The Distributed power Control (DPC)[10], proposed and tested in various works has been applied to an ad hoc network using AODV as routing scheme. To test the performance of controlled version of AODV several simulations have been performed by considering two different kinds of traffic sources and different mobility conditions. Even if in and Link State case, DPC[6] good results in terms of delivery percentage, delivery time and energy saving in several system conditions, in this paper outline that in the AODV case, its effectiveness is only performed in some operative

conditions as a consequence of the intrinsic structure of the routing protocol.

Michael Gerharz, Christian de Waal, Peter Martini(IEEE2003). In this paper, introduce statistical methods to estimate the stability of paths in a mobile wireless ad hoc environment. Identifying stable paths helps to reduce control traffic and the number of connection interruptions. By means of simulation, analyse the stability of paths chosen according to a variety of strategies, including those used by the wall-known routing protocols AODV and DSR[7], under a variety of different mobility patterns. This offers new insights into the relation be a path's stability[14] and other characteristics and shows that that our statistical metrics are able to identify stable paths in a wide range of scenarios.

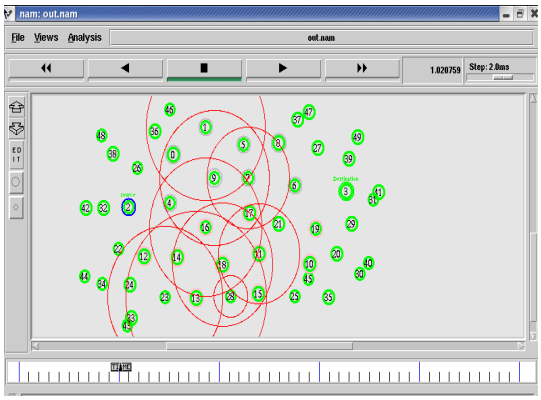
iii PERFORMANCE ANALYSIS

1 .**METRICS USED**

The performance of this system is evaluated by comparing theenergytransmission, throughput ,delay, dropratio.

2. **SIMULATION RESULTS**

Simulation is done using Network Simulator (NS) is showing the simulation model simulation occurs in a 500x500 flat gridThe simulation environment consist of 50 mobile nodes .Each communication of nodes is in 50 s and protocol used is LAER.The energy efficiency,delay,throughput,dropratio is obtained for different scenarios at different speed.



6.6.1 Energy transmission

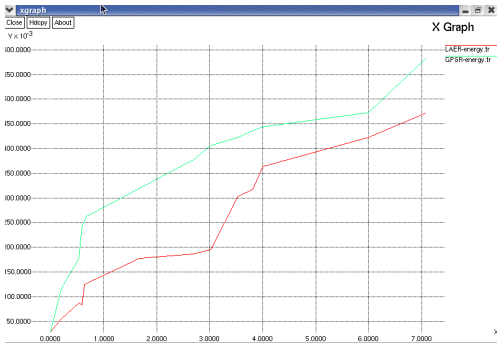


Fig :6.7Energy transmission

- Energy transmission in Greedy approach depends on large consumption of energy
- Here the LAER based approach have less energy consumption as shown in fig 6.7

6.6.2Delay

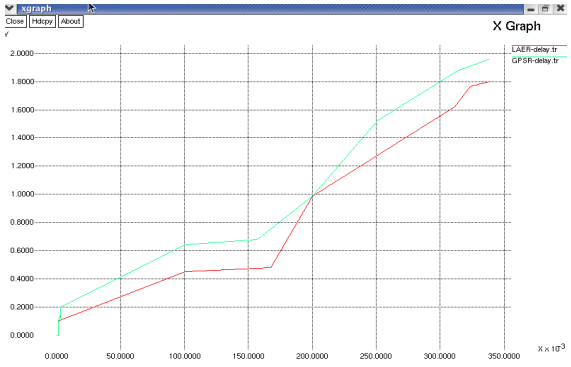


Fig 6.8 : Delay

- Here the Greedy approach consist of delay
- As it will not check whether the node is congested.
- There for delay occur in the system
- LAER consist of less delay as the neighbor node checks the information about the nodes
- Based on priority sender sends the packets

6.6.3 Throughput

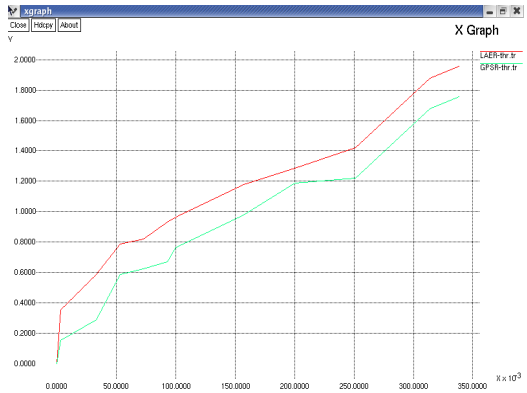


Fig 6.9 throughput

- Congested network in Greedy approach will not able to send the packets correctly
- As delay occur in the system throughput in greedy approach is not efficient
- By using LAER approach the packets will receive within the given time
- A small changes will take place in the receiver using the LAER

3.CONCLUSION AND FUTUREWORK

In this paper the comparison of both LAER and GPSR is taken for analyzing the better performance and add a cluster in LAER protocol for smallest path transmission. Future work is that to add a protocol based on lifetime.

4. REFERENCE

[1] X. H. Wei, G. L. Chen, Y. Y. Wan, and X. M. Zhang, "Longest lifetime path in mobile ad hoc networks," *J. Softw.*, vol. 17, no. 3, pp. 498–508,2006.

[10] M. Gerharz, C. de Waal, M. Frank, and P. Martini, "Link stability in mobile wireless ad hoc networks," in *Proc. 27th Annu.IEEE Conf. Local Comput.Netw.*, 2002, pp. 30–42.

[2] N. Shrestha and B. Mans, "Exploiting overhearing: Flow-aware routingfor improved lifetime in ad hoc networks," in *Proc. IEEE Int. Conf.Mobile Ad-hoc Sens. Syst.*, 2007, pp. 1–5.

[3] V. Marbukh and M. Subbarao, "Framework for maximum survivabilityrouting for a MANET," in *Proc. MILCOM*, 2000, pp. 282–286.

[4] C.-K. Toh, "Maximum battery life routing to support ubiquitous mobilecomputing in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 39,no. 6, pp. 138–147, Jun. 2001.

[5] A. Misra and S. Banerjee, "MRPC: Maximizing network lifetime for reliable routing in wireless environments," in *Proc. IEEE WCNC*, 2002,pp. 800–806.

[6] M. Maleki, K. Dantu, and M. Pedram, "Lifetime predictionrouting in mobile ad hoc networks," in *Proc. IEEE WCNC*, 2003,pp. 1185–1190.

[7] C. K. Toh, "Associativity-based routing for ad hoc mobile networks,"*Wirel. Pers. Commun.—Special Issue on Mobile Networking and ComputingSystems*, vol. 4, no. 2, pp. 103–139, Mar. 1997.

[8] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tipathi, "Signal stabilitybasedadaptive routing (SSA) for ad hoc mobile networks," *IEEE Pers.Commun.*, vol. 4, no. 1, pp. 36–45, Feb. 1997.

[9] O. Tickoo, S. Raghunath, and S. Kalyanaraman, "Route fragility: A novel metric for route selection in mobile ad hoc networks," in *Proc. IEEEICON*, 2003, pp. 537–542.

[11] L. Qin and T. Kunz, "Pro-active route maintenance in DSR," *ACM SIGMOBILE Mobile Comput.Commun. Rev.*, vol. 6, no. 3, pp. 79–89,Jul. 2002.

[12] W. Su, S. J. Lee, and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks," *Int. J. Netw.Manage.*, vol. 11, no. 1, pp. 3–30, Jan./Feb. 2001.

[13] P. Samar and S. B. Wicker, "On the behavior of communication links of a node in a multi-hop mobile environment," in *Proc. Int. Symp.MobileAd Hoc Netw. Comput.*, 2004, pp. 145–156.

[14] X. Wu, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "An analytical framework for the characterization of link dynamics in MANETs," in *Proc. IEEE Mil.Commun.Conf.*, 2006, pp.

[15] D. Johnson, Y. Hu, and D. Maltz, *DSR:RFC 4728*. [Online]. Available: http://www.ietf.org/rfc/rfc4728.txt

[16] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A survey of various propagation models for mobile communication," *IEEE Antennas Propag. Mag.*, vol. 45, no. 3, pp. 51–82, Jun. 2003.

[17] [Online]. Available: http://www.isi.edu/nsnam/ns

[18] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans.MobileComput.*, vol. 2, no. 3, pp. 257–269, Jul.–Sep. 2003.

[19] J.-Y. Le Boudec and M. Vojnovic, "Perfect simulation and stationarity of a class of mobility models," in *Proc. IEEE INFOCOM*, 2005, pp. 2743–2754.Authorized