ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

HIGH ENERGY EFFICIENT ROUTING CONSIDERING RESIDUAL ENERGY IN WIRELESS ADHOC NETWORKS

Neethumol.A[1], R.Vigneshwari[2] and R.Harish[3]
[1]*PG student, Department of ECE, Vivekanandha College of engineering for women, Tiruchengode.*
[2]*PG student, Department of ECE, Vivekanandha College of engineering for women, Tiruchengode.*
[3]*UG student, Department of EEE, Panimalar Institute of technology,Chennai.*

Abstract- This paper is based on Novel energy-aware routing algorithms proposed for wireless ad hoc networks, called reliable minimum Hybrid Dynamic Energy Routing Protocol. HDERP addresses three important requirements of ad hoc networks: energy efficiency, reliability, and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. HDERP, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. HDERP are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. we consider minute details such as energy consumed by processing elements of transceivers, limited number of retransmissions allowed per packet, packet sizes, and the impact of acknowledgment packets.

Index terms–RMECR, Energy-efficiency, Reliability, and Prolonging network lifetime, HDREP.

I.INTRODUCTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them. In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.Wireless ad-hoc network have many advantages such as low cost deployment, fast deployment, dynamic configuration. MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

II.ROUTING PROTOCOLS IN MANET

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols . However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically a "secure" protocol is only good at protecting the network against one specific type of attacks. Many researches have been done to evaluate the performance of secure routing protocols in comparison with normal routing protocols . One of the objectives of this research is to examine the additional cost of adding a security feature into non-secure routing protocols in various scenarios. The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sent, etc. It is well known that the real-world network does not operate in an ideal working environment, meaning that there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols. In the thesis, I have implemented two secure routing protocols: a secure version of the dynamic source routing - DSR (ARIADNE) and Secure Ad hoc On-demand Distance Vector routing protocol (SAODV) in the OPNET simulation environments. I will also create malicious scenarios by implementing several attacks in the simulation environments. By implementing secure routing protocols and running these two routing protocols in malicious environments, I have evaluated those secure routing protocols, and have proposed solutions to remove the weaknesses and/or to improve the performance of these secure routing protocols.Routing protocols in ad hoc mobile wireless network can generally be divided into three groups.

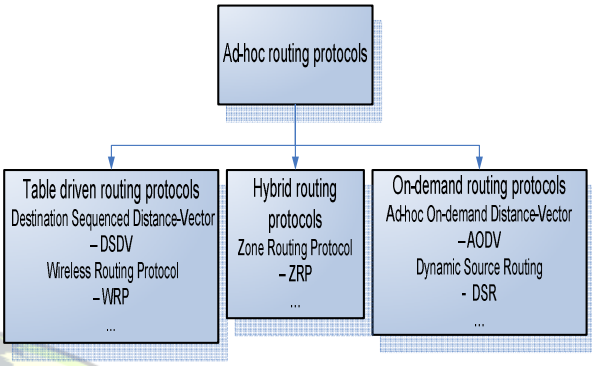


Figure 1: Hierarchy of ad-hoc routing protocols

The two of the most common routing protocols used in mobile ad hoc network: Dynamic Source Routing protocol (DSR) and Ad hoc On-demand Distance Vector routing protocol (AODV) .

III.CURRENT CHALLENGES IN MANET

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing. This thesis focuses mainly on routing issues in ad hoc networks. Some of the other issues in adhoc networks are distributed network, dynamic topology, power awareness, addressing scheme, network size, security.

A MANET is a distributed wireless network without any fixed infrastructure. Christo Ananth et al. [2] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. Security in an ad hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation - are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets.

IV. PROTOCOL SYSTEM

A.EXISTING PROTOCOL SYSTEM

RMECR addresses three important requirements of ad hoc networks: energy-efficiency, reliability, and prolonging network lifetime. It considers the energy consumption and the remaining battery energy of nodes as well as quality of links to find energy-efficient and reliable routes that increase the operational lifetime of the network. RMER, on the other hand, is an energy-efficient routing algorithm which finds routes minimizing the total energy required for end-to-end packet traversal. RMER and RMECR are proposed for networks in which either hop-by-hop or end-to-end retransmissions ensure reliability. Simulation studies show that RMECR is able to find energy-efficient and reliable routes similar to RMER, while also extending the operational lifetime of the network. This makes RMECR an elegant solution to increase energy-efficiency, reliability, and lifetime of wireless ad hoc networks. In the design of RMECR, we consider minute details such as energy consumed by processing elements of transceivers, limited number of retransmissions allowed per packet, packet sizes, and the impact of acknowledgment packets.This negatively affects energy-efficiency, reliability, and the operational lifetime of the network altogether. Discovered routes by these algorithms may neither be energy-efficient nor be reliable.This can increase the overall energy consumption in the network. The network lifetime may be reduced.

B. PROPOSED PROTOCOL SYSTEM

Propose a novel energy-aware routing algorithm, called Hybrid Dynamic Energy Routing Protocol (HDERP). HDERP finds energy efficient and reliable routes that increase the operational lifetime of the network. HDERP is proposed for networks with hop-by-hop (HBH) retransmissions providing link layer reliability, and networks with E2E retransmissions providing E2E reliability.Considers energy efficiency, reliability, and prolonging the network lifetime in wireless ad hoc networks. Energy consumption of processing elements of transceivers is considered. HDERP extends the operational lifetime of the network .It finds reliable routes.The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

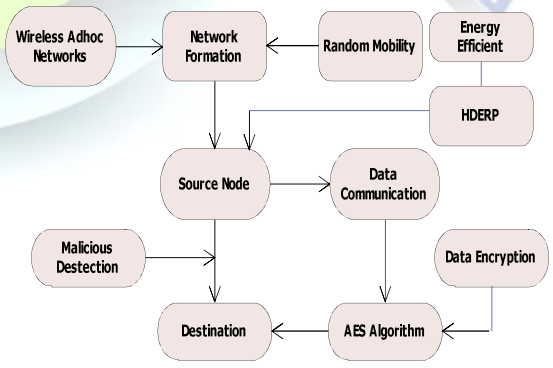


Figure 2: Data flow diagram

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

C.NETWORK SIMULATOR

A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modeled with devices, traffic etc and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as WLAN, Wi-Max, UDP, and TCP.

Most of the commercial simulators are GUI driven, while some network simulators require input scripts or commands (network parameters). The network parameters describe the state of the network (node placement, existing links) and the events (data transmissions, link failures, etc). Important outputs of simulations are the trace files. Trace files can document every event that occurred in the simulation and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week,month, in order to reflect average, worst-case, and best-case conditions. Network simulators can also provide other tools to facilitate visual analysis of trends and potential trouble spots.

D.SAMPLE CODING

```
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in ifq
set val(nn)     30                         ;# number of mobilenodes
set val(rp)     AODV                       ;# routing protocol
set val(rp1)    HDERP                      ;#routing protocol
set val(x)      1000                       ;# X dimension of topography
set val(y)      550                        ;# Y dimension of topography
set val(stop)   15.0                       ;# time of simulation end
set ns [new Simulator]
```

V. SIMULATION RESULTS

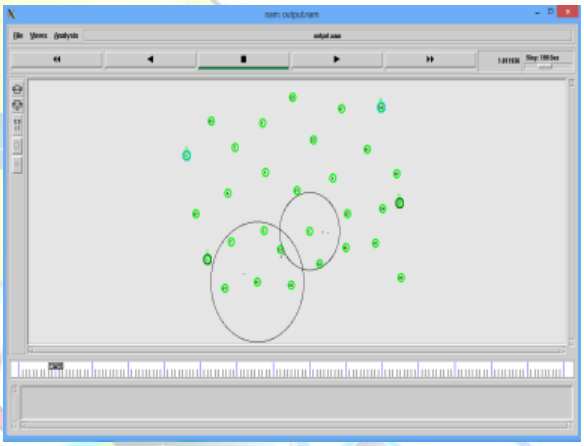


Figure 3: Shortest path in the network

Routing is the process of building up the tables that allow the packets on the intermediate nodes between source and destination.

The proposed algorithm finds the shortest path in the network.. The blue and black source and destination node on unicast routing(single sender and single receiver)in the network and also transmission of packets through the shortest path in the network.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

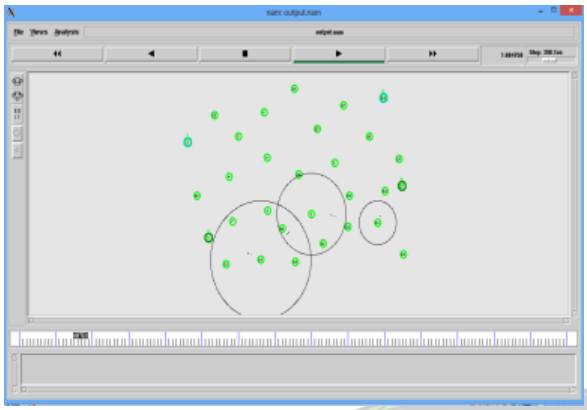


Figure 4: Transmission of packets

The simulation shows transmission of packets between the source and destination through the shortest intermediate nodes.

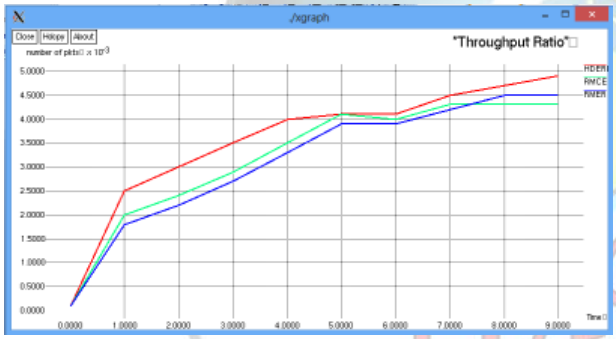


Figure 5: Number of packets Vs Time

Throughtput in a network is the number of packets passing through the network in a unit of time.The graph that the number of packets increases with the time. And throughput ratio increased in the proposed system(HDREP).

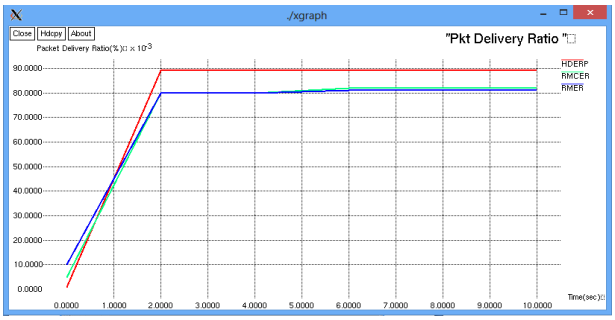


Figure 6: Packet delivery ratio Vs Time

Packet delivery ratio defines the ratio of number of packets transmitted to the number of packets received. And the packet delivery increases with the time.

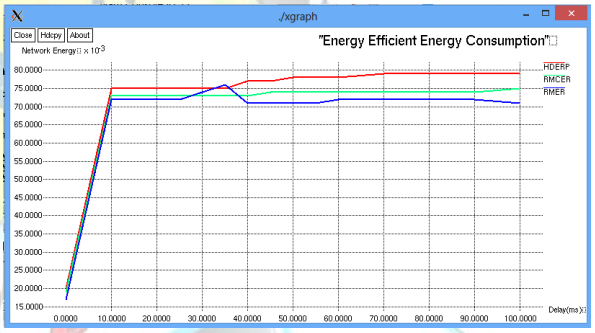
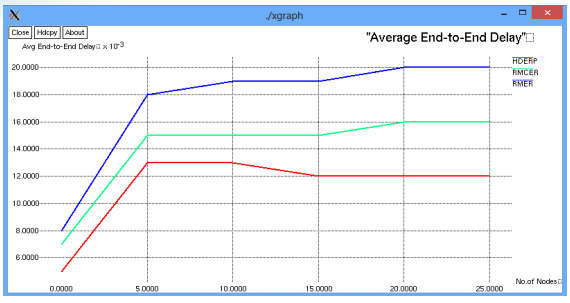


Figure 7: Network energy Vs Delay

Energy efficient is an mechanism for reducing energy cost of data communication in wireless adhoc networks. That the network energy increases with the decrease in delay.And the network energy is increased in the proposed system(HDREP).



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

Figure 8: Average end to end Vs Number of nodes

Average end to end delay increases with the number of node.. The average end to end delay increases in the proposed system(HDREP) with the number of nodes.

VI. CONCLUSION

We presented an in-depth study of energy-aware routing in ad hoc networks, and we proposed a new routing algorithm for wireless ad hoc networks, namely, reliable minimum energy cost routing (RMECR). RMECR can increase the operational lifetime of the network using energy-efficient and reliable routes. In the design of RMECR, we used a detailed energy consumption model for packet transfer in wireless ad hoc networks. RMECR was designed for two types of networks: those in which hop-by-hop retransmissions ensure reliability and those in which end-to-end retransmissions ensure reliability. The general approach that we used in the design of RMECR was used to also devise a state-of-the-art energy-efficient routing algorithm for wireless ad hoc networks, i.e., reliable minimum energy routing (RMER). RMER finds routes minimizing the energy consumed for packet traversal. RMER does not consider the remaining battery energy of nodes, and was used as a benchmark to study the energy-efficiency of the RMECR algorithm. Extensive simulations showed that RMER not only saves more energy compared to existing energy efficient routing algorithms, but also increases the reliability of wireless ad hoc networks.we conclude that HDREP has better efficiency then RMECR and RMER.

VII.REFERENCES

[1] X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and Energy-Efficient Routing for Static Wireless Ad Hoc Networks with Unreliable Links," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 10, pp. 1408-1421, Oct. 2009.

[2] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[3] X. Li, H. Chen, Y. Shu, X. Chu, and Y.-W. Wu, "Energy Efficient Routing with Unreliable Links in Wireless Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '06), pp. 160-169,2006.

[4] Q. Dong, S. Banerjee, M. Adler, and A. Misra, "Minimum Energy Reliable Paths Using Unreliable Wireless Links," Proc. ACM MobiHoc, pp. 449-459, May 2005.

[5] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[6] D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High Throughput Path Metric for Multi-Hop Wireless Routing," Proc. ACM MobiCom, pp. 134-146, 2003.

[7] J. Gomez, A.T. Campbell, M. Naghshineh, and C. Bisdikian, "PARO: Supporting Dynamic Power Controlled Routing in Wireless Ad Hoc Networks," Wireless Networks, vol. 9, no. 5, pp. 443-460, 2003.

[8] D. Kim, J.J.G. Luna Aceves, K. Obraczka, J. Carlos Cano, and P. Manzoni, "Routing Mechanisms for Mobile Ad Hoc Networks Based on the Energy Drain Rate," IEEE Trans. Mobile Computing, vol. 2, no. 2, pp. 161-173, Apr.-June 2003.

[9] S. Banerjee and A. Misra, "Minimum Energy Paths for Reliable Communication in Multi-Hop Wireless Networks," Proc. ACM MobiHoc, pp. 146-156, June 2002.

[10] C. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 39, no. 6, pp. 138-147, June 2001.

[11] S. Singh and C. Raghavendra, "PAMAS—Power Aware Multi Access Protocol with Signalling for Ad Hoc

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 22, April 2016

Networks," ACM Computer Comm. Rev., vol. 28, pp. 5-26, 1999.

[12] S. Singh, M. Woo, and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Proc. ACM MobiCom, Oct. 1998.