iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1094

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

A Review of Modern Adaptive Routing Algorithm for Wireless ADHOC N/W

Ms. Vaishali Matvankar[1], Mr. Mayur Rathi[2], Mr. Mayank Bhatt[3]
[1, 2, 3]*Computer Science and Engineering, LNCTS, RIT Indore,*

Abstract: ***Adaptive opportunistic routing is a heart favorite's topic for many researchers. In this synopsis, we are presenting a review of some modern adaptive opportunistic scheme for the wireless ADHOC network. In comparison to cellular networks the ad hoc networks are more adaptable to changing physical conditions and traffic demands. The attenuation characteristics of the media are nonlinear due to the unpredictability of the wireless medium. The energy efficiency will be superior and increased special diversity will yield superior capacity and hence superior spectral efficiency.***
Keywords: Adaptive opportunistic Routing, Data redundancy, Spectral efficiency, Dynamic Routing, synchronization control.

I. INTRODUCTION

The Ad hoc wireless networks are created by devices which are able to communicate with each other via the wireless medium without having to resort to a pre-existing infrastructure. The Wireless ad hoc networks also commonly known as Mobile Ad Hoc Networks (MANETs) can form stand-alone sets of wireless terminals. At the same time these terminals could also be sometimes connected to a cellular system or to a fixed network. The basic feature of the ad hoc networks is that they are self-configuring dynamic networks that do not require the intervention of a centralized administration. It should not be considered that terminals within the ad hoc networks can only function as end systems with the end station only executing the applications. The terminals in the ad hoc networks can function as intermediate nodes where they come into play by forwarding packets for other nodes. Therefore, there is the possibility of two nodes communicating, even in the case when they reside outside each others transmission ranges becomes possible because intermediate nodes existing within the ad hoc network can function as routers. Because of this reason the wireless ad hoc networks are termed as multi hop wireless networks.

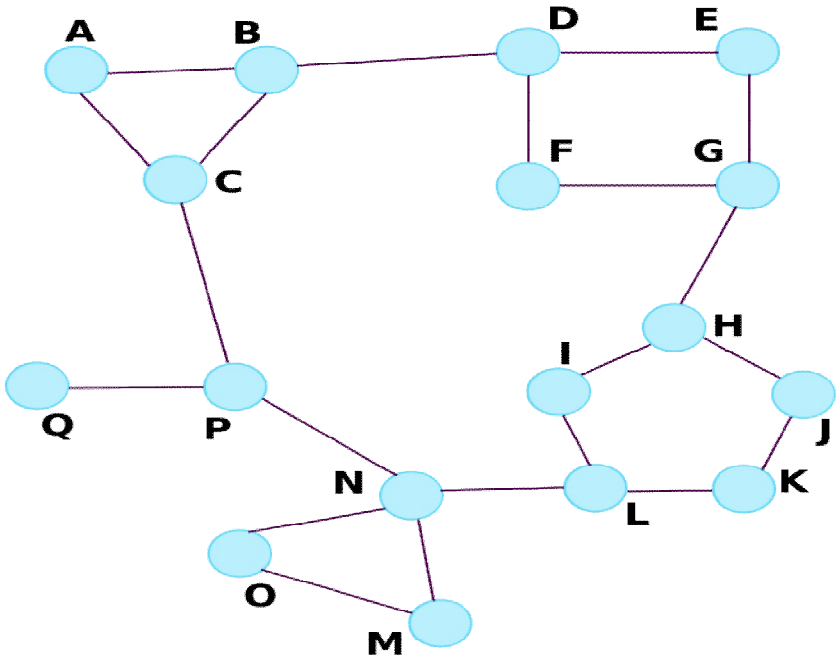


Figure 1: Routing Example

This is a routing technique in which all the sensor nodes play the same roles, such as collecting data and communicating with the sink, i.e. all the data collected in the remote area can be same or duplicated as all the sensor nodes work in the same way. Flat routing protocols distribute information as needed to any reachable sensor node within the sensor cloud.

In this routing technique all the routing sensors in the network are clustered and a cluster head collects and aggregates the data and checks for redundancy of the data that is collected before it is sent to the sink. Energy depletion will be strongest in that head. This saves communication and processing work and also saves energy.

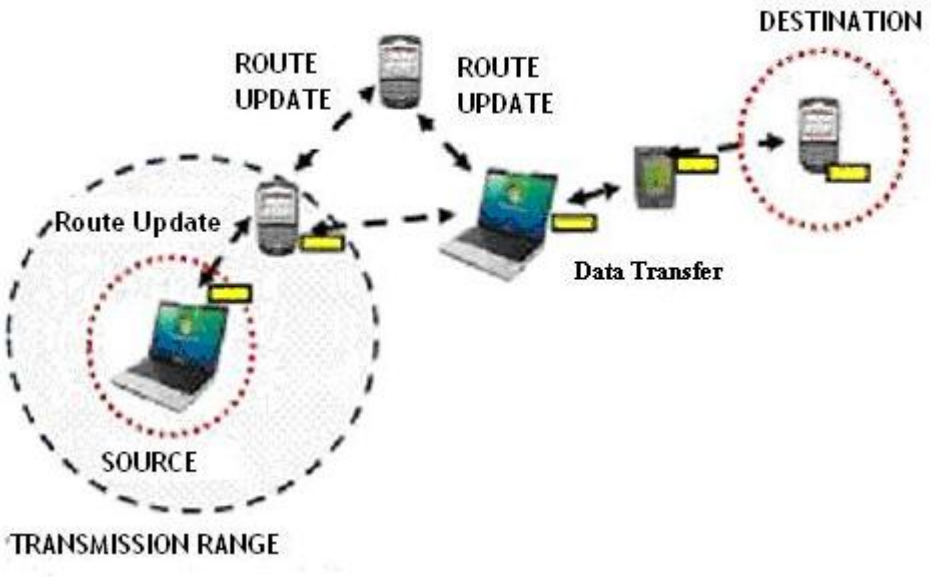


Figure 2 : Adaptive Routing Concept

In location-based routing, all the sensor nodes are addressed by using their locations. Depending upon the strength of the incoming signals, it is possible to calculate the nearest neighbor node's distance. Due to obstacles in the network often the signal strength becomes weaker and nodes find it difficulty in finding the nearest neighbor nodes. All the nodes in the network exchange this data in order to know about neighboring nodes. This is useful for communicating and transferring information. As energy is the major factor of concern in routing protocols, location-based schemes demand that nodes should change their state from active to sleep mode when there is no activity. The more nodes in sleep mode, the more energy is saved.

In comparison to cellular networks the ad hoc networks are more adaptable to changing physical conditions and traffic demands. The attenuation characteristics of the media are nonlinear due to the unpredictability of the wireless medium. The energy efficiency will be superior and increased special diversity will yield superior capacity and hence superior spectral efficiency. All these features make the ad hoc networks suitable for pervasive communications. A concept that is closely affiliated with 4G architectures and heterogeneous networks. The flexibility at various levels for instance distributed medium access control or dynamic routing poses new challenges in wireless ad hoc networks.

II. LITERATURE SURVEY

The authors A. Menaka Pushpaet. al. introduced a perfect trust model in the network layer and established secure route between source and destination without any intruders or malicious nodes. The existing AODV routing protocol has been modified in order to adapt the trust based communication feature. The proposed trust based routing protocol is equally concentrates both in node trust and route trust. The route trust plays an equal role with node trust. By using trust value the secure route can be established in the MANET. Here, the network security enhancement is completely performed in the lime light of trust value. In dynamic environment, the node can change its characteristics at any time. After the successful participation in the route establishment process, neighbor may behave like as a malicious node. To avoid this, the route trust process continuously monitors the active routes and calculates the current route trust value or the status of the route. Most of the previous works have been concentrated only in the node trust for establishing communication. This paper outlines three main operations; The Node trust calculation, The Route trust calculation and The Trust based route establishment and route monitoring process. Proposed model requires some adequate changes in the existing source initiated routing protocol. The modified AODV routing protocol establishes route among nodes based on the trust value.

Using simulation results the performance of this protocol is not sufficient justified. In future, AODV will be incorporate with other MANET routing protocols [1].

Authors Wenchao Huang, Yan Xiong, Depin Chen et. al. proposed a novel secure routing protocol DAAODV which is based on Ad-hoc On-demand Distance Vector routing (AODV). The DAAODV takes full advantage of trusted computing technology. It takes advantage of particularly the Direct Anonymous Attestation (DAA) and Property-based Attestation (PBA) protocols. The DAAODV is an anonymous protocol without requirement of Trusted Third Party (TTP). Authors propose an efficient signing and verification scheme to overcome the potential DoS attacks triggered by the low efficiency of DAA and PBA. The simulation results show that DAAODV is still efficient in discovering secure routes compared with AODV protocol. This paper presents a novel secure ad hoc routing protocol DAAODV which is anonymous and avoids TTP and prevents from malicious nodes and selfish nodes. It is using Direct Anonymous Attestation (DAA) to accomplish full anonymity in the routing protocol and use issuer instead of TTP. The main challenges in implementing this protocol is the cost of DAA and PBA protocol is a little high, therefore we choose an efficient DAA protocol and propose a new light weighted signing and verifying protocol to ease the problem. Experiments proves that it is still very efficient compared with AODV protocol.

The DAAODV presents almost a fully protection of routing process and it can be more easily analyzed than other protocols for the hosts that could participate in the routing protocol have to run in an anticipated way. Extra cost of DAAODV via AODV is the establishment of secure link which uses DAA and PBA protocols. The DAA presented in this paper is very efficient in DA A Sign and DAA Verify though not efficient in join protocols. The future work is to make a fine-grained construction of the routing software, because the design of DAAODV on software level is a little coarse-grained. For example, there should be a concrete scheme of operating the PCRs, also it should prove that the DAAODV can avoid attacks at the software level [2].

The Cuirong Wang, Shuxin Cai et. al. proposed a secure routing protocol based on multipath routing technology, namely AODVsec. It divides a data unit into several data pieces and transmits these pieces through different paths. After setting security level on each node, the AODVsec limits the maximum number of data pieces an intermediate node can forward. Therefore, the malicious node cannot get enough data information for breaking the encryption algorithm. The simulation results show that AODVsec improves security with negligible routing overhead by comparison of the traditional multipath AODV routing protocols.The simulation results show that AODVsec outperforms traditional multipath routing on ensuring security. As a common case, the attacker cannot intercept all the paths, the AODVsec avoids maliciously accessing a entire data packet, so AODVsec improves system's security with negligible routing overhead. It still has some imperfect points. It is required need to focus on designing the synchronization control mechanism to solve this problem [3].The authors Zeyad M. Alfawaer and SaleemAl_zoubiet. al. proposed an effective security AODV algorithm called ES-AODV to enhance the data security. The experimental results show that the proposed algorithm provides a reasonably good level of security and performance. The main objective of this algorithm is to provide a secure solution for communication in ad hoc network applications strong enough to withstand an active internal threat within the network. The proposed protocol will be able to find a trusted end-to-end route free of any malicious entity, also effectively isolating any node trying to inject malicious information into the network. This protocol is based on the following assumptions. The main focus is on the network layer and the protocol that we propose here is an extension of the Ad hoc On Demand Distance Vector routing protocol which we call effective security AODV commonly ES-AODV. We assume that all the nodes are identical in their physical characteristics and all communicate via a shared wireless channel and operate in a promiscuous mode. It is a reliable link layer protocol.

Efficient security algorithm ES-AODV enhances the security in ad hoc wireless networks. But the routing protocol performs Does not better than the existing secure AODV routing protocol with increased mobility in the network. This should be improve in future extension [4].

The work done by Muhammad Naeemv, ZahirAhmed , Rashid Mahmood and Muhammad Ajmal Azad et. al. evaluated the two secure routing protocols Ariadne and SAODV in the performance aspects instead of security aspects under Random Way Point and Manhattan Grid mobility models. They implemented the extension of AODV that is Secure Adhoc on-Demand Distance Vector routing protocol SAODV and the extension of DSR that is Ariadne in the Network Simulator 2. There result is compared on the basis of following quality of service parameters like delay, routing overhead ,jitter, throughput.

In future it is requireed more specifically SAODV to decrease the processing requirements to tackle hash chains and digital signatures to implement the security [5].

The authors PreetiBhati, Rinki Chauhan and R K Rathyet. Al tried to remove the existence of misbehaving nodes that may paralyze or slows down the routing operation in MANET. It increases the efficiency of a network. The efficiency can be calculated by the parameters or factors such as transmission capacity battery power and scalability. Proposed method is considering the most crucial

factor named as transmission capacity of a node. In MANET, when the network size increases complexity of a network also increases. To overcome this problem they make network as modular. Therefore the network becomes task specific which refer to a particular work only. This proposed protocol provides the most efficient and reliable route which may or may not be minimum hop count. But the transmission capacity factor into the networking as MANET of the protocol will need to improve in future [6].

III.CONCLUSION

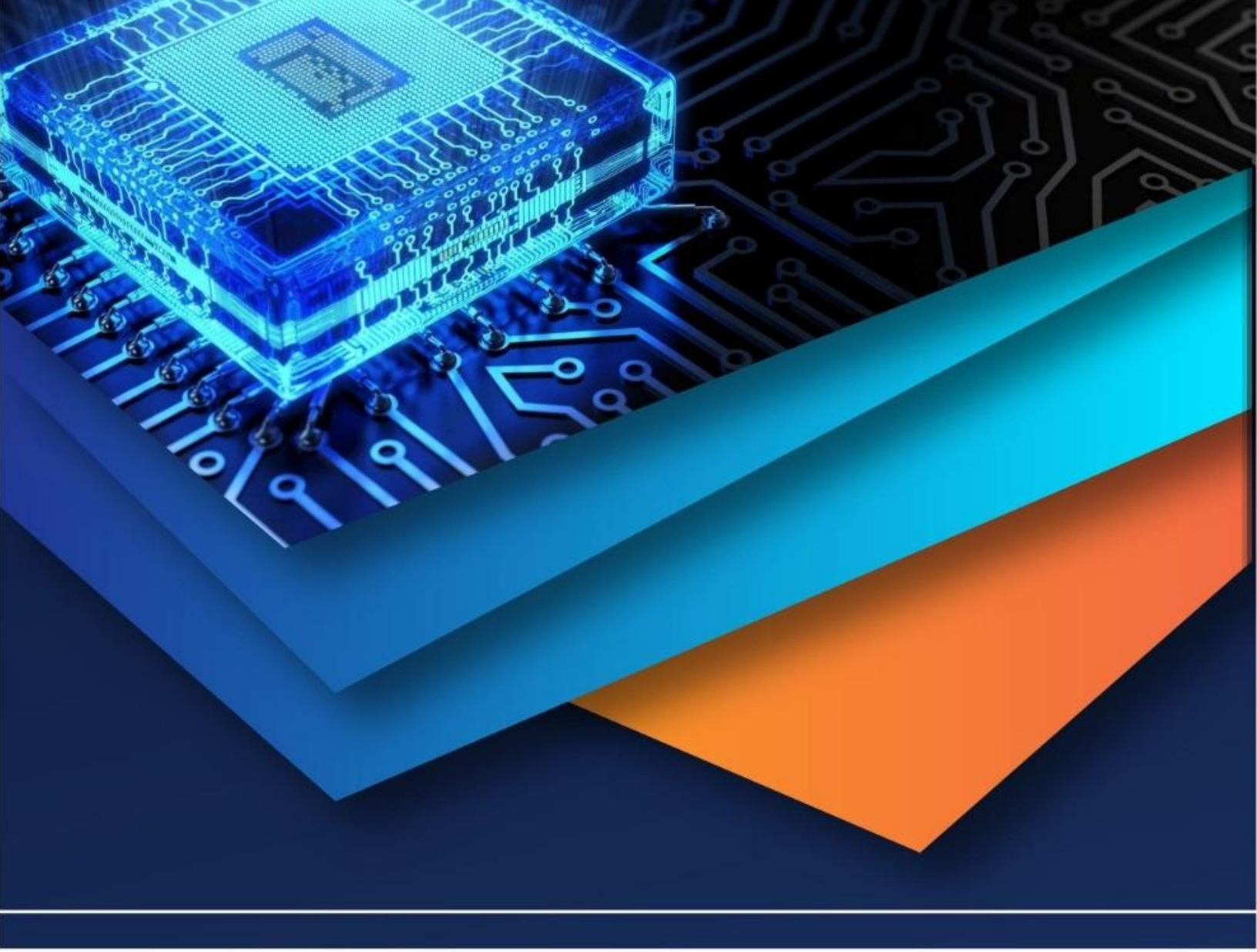
Adaptive opportunistic routing in wireless network is a burning research topic. This paper presents a review of the most popular methods for the adaptive opportunistic routing. It is basically a comprehensive survey over the routing in the adhoc network. The working of each method is given in brief. The pros and cons of each method are also discussed in brief.

IV. ACKNOWLEDGMENT

It gives me immense and satisfaction in publishing this research paper. So it becomes my duty and pleasure to express my deep regards to them.
On the outset of this research paper I express my sincere regards to my guide MR. MAYUR RATHI , MR.MAYANK BHATT who gave me an opportunity to work upon this topic and made me present my views and my ideas on topic through this paper.
I alsothank to all faculty members of CSE department (RIT), as they have been helping me in it, without their support, working on the paper would have been very difficult.

REFERENCES

[1] A.MenakaPushpa, “Trust Based Secure Routing in AODV Routing Protocol”, IEEE 2009.
[2] Wenchao Huang, Yan Xiong, Depin Chen, “DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation”, 2009 International Conference on Computational Science and Engineering, IEEE 2009, pp. 809-916.
[3] Cuirong Wang, ShuxinCai, and Rui Li, “AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security”, 2009 International Conference on Multimedia Information Networking and Security, IEEE 2009, pp. 401-404.
[4] Zeyad M. Alfawaer and SaleemAl_zoubi, “A proposed Security subsystem for Ad Hoc Wireless Networks”, 2009 International Forum on Computer Science-Technology and Applications, IEEE Computer Society 2009, pp. 253-255.
[5] Muhammad Naeemv, Zahir Ahmed, Rashid Mahmood, and Muhammad Ajmal Azad, “QOS Based Performance Evaluation of Secure On-Demand Routing Protocols for MANET's”, 20 1O IEEE, ICWCSC 2010X.
[6] PreetiBhati, RinkiChauhan and R K Rathy, “An Efficient Agent-Based AODV Routing Protocol in MANET”, International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 7 July 2011, pp. 2668-2673.
[7] Ming Yu, Mengchu Zhou, and Wei Su, “A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009, pp. 449-460.
[8] D. Suganya Devi and Dr. G.Padmavathi, “IMPACT OF MOBILITY FOR QOS BASED SECURE MANET”, International journal on applications of graph theory in wireless ad hoc networks and sensor networks, pp. 46-57
[9] R. R. Choudhury, “Brownian gossip: Exploiting node mobility to diffuse information in ad hoc networks,” in Proc. Int. Conf. Collaborative Comput.: Netw., Appl. Worksharing, 2005, pp. 1–5.
[10] T. Hara and S. K. Madria, “Consistent Management Strategies for Data Replication in Mobile Ad hoc Networks,” IEEE Transactions on Mobile Computing, vol. 8, no. 7, July 2009, pp. 950-967.
[11] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini, “Modeling mobility in disaster area scenarios,” Perform. Eval., vol. 66, no. 12, pp. 773–790, Dec. 2009.
[12] M. Asplund and S. Nadjm-Tehrani, “A partition-tolerant manycast algorithm for disaster area networks,” in Proc. 28th Int. Symp. Reliable Distrib. Syst., 2009, pp. 156– 165.
[13] M. B. Donley and N. A. Schwartz, United States Air Force Unmanned Aircraft Systems Flight Plan 2009– 2047, 2009. [Online]. Available: http://handle.dtic.mil/100.2/ADA505168
[14] P.-C. Cheng, K. C. Lee, M. Gerla, and J. Härri, “GeoDTN+Nav: Geographic DTN routing with navigator prediction for urban vehicular environments,” Mobile Netw. Appl., vol. 15, no. 1, pp. 61–82, Feb. 2010.
[15] J. LeBrun, C. Chuah, D. Ghosal, and M. Zhang, “Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks,” in Proc. IEEE 61st Veh. Technol. Conf., 2005, pp. 2289–2293.
[16] S. M. Das, H. Pucha, and Y. C. Hu, “Performance comparison of scalable location services for geographic ad hoc routing,” in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc., 2005, pp. 1228–1239.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY