A DISTRIBUTED ADAPTIVE ROUTING ALGORITHM FOR WIRELESS ADHOC NETWORK

Ms. Vaishali Matvankar [1] Mr. Hemant Gupta[2]

Computer Science and Engineering, LNCTS (RIT) Indore,

ABSTRACT:

Adaptive opportunistic routing is a heart favorite topic for many researchers. In this paper, 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. By using a reinforcement learning framework, we will propose an adaptive opportunistic routing algorithm which minimizes the expected average per packet cost for routing a packet from a source node to a destination. It results in avoiding unnecessary packet retransmission.

Keywords: Adaptive Opportunistic Routing, Adhoc Network, Reinforcement learning,

1. 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.

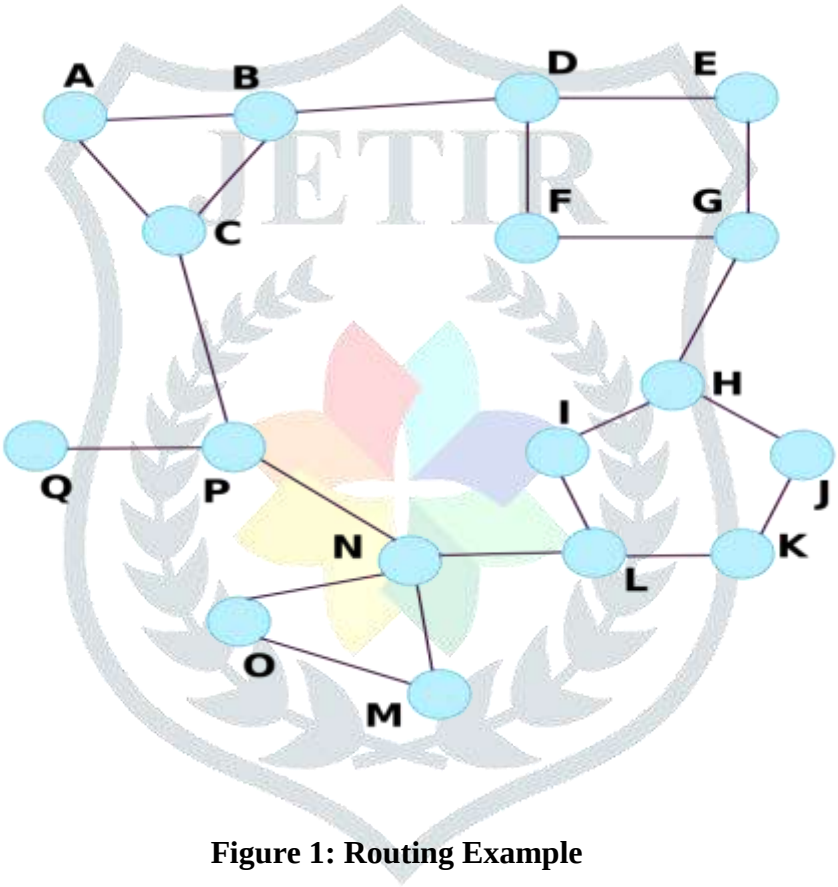

Figure 1: Routing Example

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.

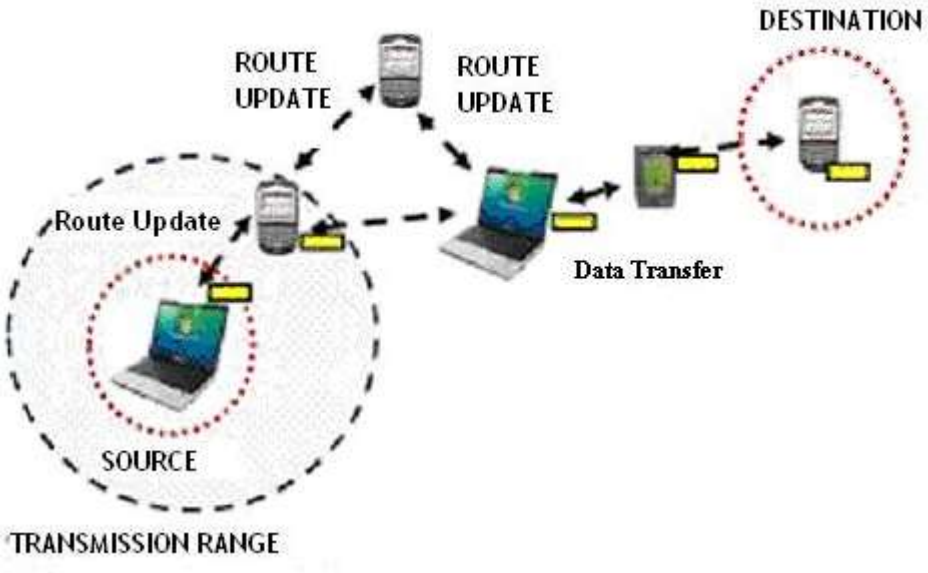

Figure 2: Adaptive Routing Concept

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.

The opportunistic routing decisions, in contrast, are made in an online manner by choosing the next relay based on the actual transmission outcomes as well as a rank ordering of neighboring

nodes. Opportunistic routing mitigates the impact of poor wireless links by exploiting the broadcast nature of wireless transmissions and the path diversity.

Traditional routing protocols that send traffic on predetermined paths face problems due to the unreliability of wireless links. To cope with this unpredictability of the wireless medium, a new routing paradigm has been recently proposed by researchers, termed as opportunistic routing [7],[8],[9]. Opportunistic routing is different from the traditional routing schemes in that it exploits the spatial diversity and broad cast nature of the wireless medium. It also differs in its route selection after packet transmissions i.e. forwarders of a packet are chosen amongst the recipients after the packets transmission. These features allow opportunistic routing to unite several weak links into a strong one as well as take advantage of unanticipated long or short transmission, thus allowing coping well with the unpredictable wireless medium [10].

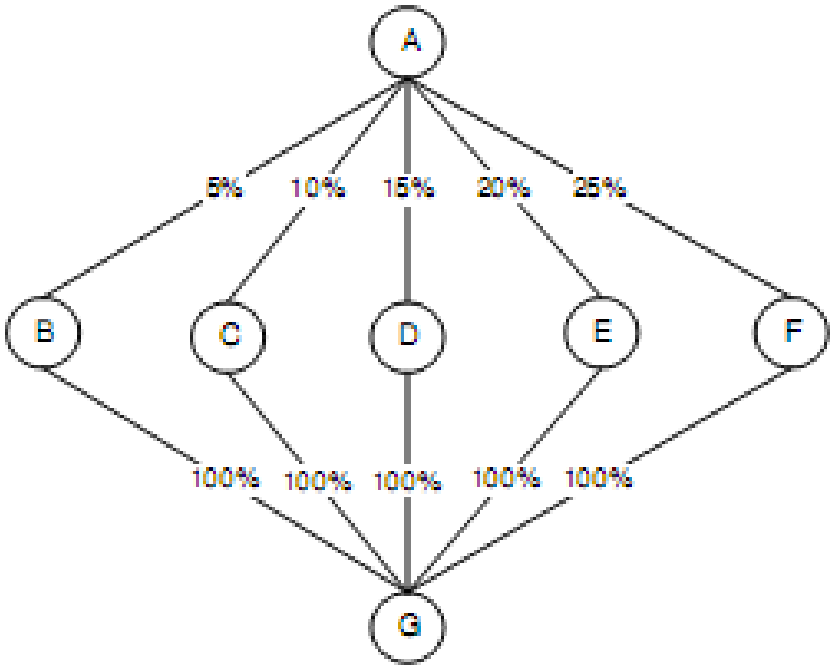

Figure3: Opportunistic routing combining multiple weak links into a strong one

In order to understand how opportunistic routing combines weak links to make stronger ones consider the system in the above figure 3. A wireless network source node (A) is connected to five intermediate nodes (BF) via wireless links. Because of the unpredictable nature of the wireless medium we assume that each of the five intermediate links are weak and have different delivery rates. Let these delivery rates be 5, 10, 15, 20 and 25 percent for links A-B, A-C, A-D, A-E, and A-F respectively. To simplify the scenario we assume independent loss rates for

each link. Furthermore, each intermediate link has 100 percent delivery rate to the destination i.e. node G.

2. LITERATURE SURVEY

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].

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 DAASign and DAAVerify 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 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].

[4] 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].

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

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].

The conventional routing in ad hoc networks attempts to find a fixed path along which the packets are forwarded. The existing routing algorithms are inspired by the classical routing. In classical routing a fixed path is established. Such fixed path based routing scheme fail to take advantage of broadcast nature and opportunities provided by the wireless medium and then it results in unnecessary packet retransmissions.

The correspondence procedure among sensor hubs is administrated by steering conventions; in this way the general execution of the any remote system for the most part relies on supportive directing methodology. Numerous quantities of vitality proficient and secure directing conventions have been planned and actualized for different application administrations so as to improve the correspondence execution of the WSNs [11] [12].

The most noticeable review papers [13] concentrated on security issues. Nonetheless, as for security concerns none of the exploration study gave productive arrangement till now, this overview study infer that it was very provoking assignment to comprehend the adequacy of the earlier methods. The examination unequivocally accept that security highlights can be

fused with different boundaries including delay, transmission capacity, vitality and so forth, and it isn't important to incorporate cryptography conspires as it were.

The latest [14], proposed a versatile directing instrument for WSNs, which is answerable for upgrading the WSNs execution utilizing the dynamic multi-steering plan. The point was to locate the most limited way among every hub to the sink hub. Because of this, it can devour less power and keep up the force utilization all through the system by transmitting the restricted information bundles for each hub. Moreover, it can lessen the information repetition at the transmission procedure.

Creators in [15] proposed vitality adjusted directing convention for WSNs. They embraced the fluffy rationale and k-implies bunching way to deal with delay the system lifetime. Additionally, they planned a hereditary calculation to acquire the fluffy guideline for different sizes of sensor systems.

2.1 DISADVANTAGES OF EXISTING SYSTEM:

Such fixed path schemes fail to take advantages of broadcast nature and opportunities provided by the wireless medium and result in unnecessary packet retransmissions. The opportunistic routing decisions, in contrast, are made in an online manner by choosing the next relay based on the actual transmission outcomes as well as a rank ordering of neighboring nodes. Opportunistic routing mitigates the impact of poor wireless links by exploiting the broadcast nature of wireless transmissions and the path diversity.

3. PROPOSED METHODOLOGY:

We have investigated the problem of opportunistically routing packets in a wireless multi-hop network when zero or erroneous knowledge of transmission success probabilities and network topology is available. By using a reinforcement learning framework, we will propose an adaptive opportunistic routing algorithm which minimizes the expected average per packet cost for routing a packet from a source node to a destination.

The stages of the proposed scheme are as follows:

- The Initialization stage
- The Transmission Stage
- The Acknowledgement Message Passing
- The Relay Stage

- **Initialization stage**

We consider the routing of packets from a source node 0 to a destination node d in a wireless ad-hoc network or mobile ad hoc network of d + 1 nodes

- **Transmission Stage**

We will assume a fixed transmission cost pi > 0 is incurred upon a transmission from node i. The transmission cost pi can be considered to model the amount of energy used for transmission, or the expected time to transmit a given packet, or hop count when the cost is equal to unity.

- **Acknowledgement Message Passing**

The termination events are discriminated as follows: it is assumed that upon the termination of a packet at the destination or successful delivery of a packet to the destination a fixed and given positive reward R is obtained, otherwise no reward is obtained if the packet is terminated or dropped before it reaches the destination.

- **Relay Stage**

We are given a successful transmission from node i to the set of neighbor nodes S, the next routing decision includes

- retransmission by node i,
- relaying the packet by a node j 2 S
- Dropping the packet all together. If node j is selected as a relay then it transmits the packet at the next slot while other nodes remove that packet.

4. RESULTS:

Our proposed scheme results in low complexity, low computational overhead, and distributed asynchronous implementation in comparison to the existing methods of routing. The most important characteristics of the proposed solution are:

- It will minimize the expected average per packet cost for routing a packet from a source node to a destination.
- It is unaware to the initial knowledge of network.
- It is distributed. Therefore, each node makes decisions based on its belief using the information obtained from its neighbors.
- It is asynchronous. Therefore, at any time any subset of nodes can update their corresponding beliefs.

Comparison Table:

Proposed Framework	Existing framework[16]
• It is distributed. Therefore each node makes decisions based on its belief using the information obtained from its neighbors.	• It is not distributed. Therefore each node cannot make decisions based on its belief using the information obtained from its neighbors.
• It is asynchronous. Therefore at any time any subset of nodes can update their corresponding beliefs.	• It is synchronous. Therefore any subset of nodes cannot update their corresponding beliefs.
• It is unaware to the initial knowledge of network.	• It is aware to the initial knowledge of network.

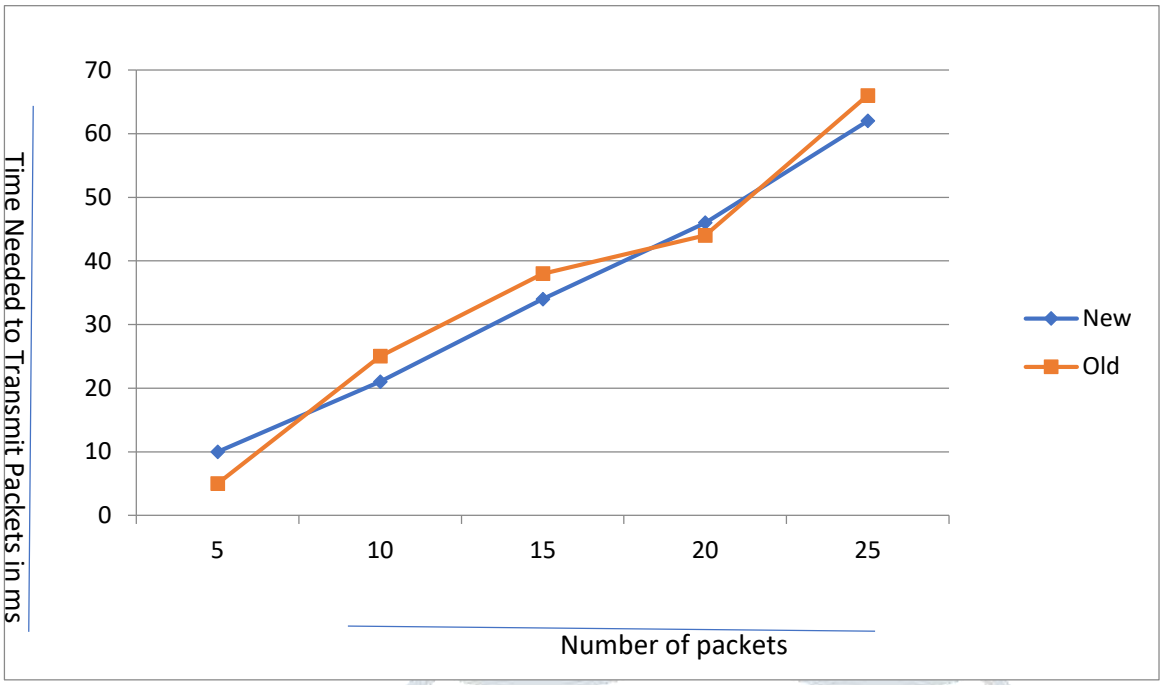

Figure 4 Time needed to Transfer packets

From above diagram, it is clear that the new algorithm perform better than the previous method in terms of computational time.

5. 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. Reinforcement based adaptive opportunistic method routing is proposed. The proposed distributed opportunistic routing method is better. As it is asynchronous and distributed. It will reduce average per packet cost during transmission.

REFERENCES:

[1] A.Menaka Pushpa, "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, Shuxin Cai, 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 Saleem Al_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, Zah ir 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] Preeti Bhati, Rinki Chauhan 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] S. Omar, O. E. Ghandour, and A. M. A. E-Haleem, "Multipath Active Based Routing Protocol for Mobile cognitive Radio AdHoc Networks", Wireless Communications and Mobile Computing, 2017.

[12] G. Nandini, J. Anitha, "Performance Chronicles of Multicast Routing Protocol in Wireless Sensor Network", International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp.284-293, 2017

[13] H. Singh and D. Singh, "Taxonomy of routing protocols in wireless sensor networks: A survey", In 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 822-830, 2016

[14] F. E-Hajji, C. Leghris, and K. Douzi, "Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks", Journal of Communications and Information Networks 3, no. 1 (2018): 67-83

[15] L. Li, and D. Li. "An Energy-Balanced Routing Protocol for a Wireless Sensor Network." Journal of Sensors, 2018

[16] B Narsimhan and R vadivel, "Adaptive Position based Reliable Routing Protocol(APBRRP) for Mobile Ad Hoc Networks, IJCA, august 2012.