International Journal of Scientific Research & Engineering Trends
Volume 9, Issue 3, May-Jun-2023, ISSN (Online): 2395-566X

Novel Approach To Wsn Pdr Enhancement In Manet Routing Control Approach

Diksha Yadav, Prof. Amit Thakur
School Of Engineering and Technology, Vikram University, Ujjain
University in Ujjain, Madhya Pradesh

Abstract- Mobile device users use their devices any time anywhere. Hence there are different constraints we discussed on routing in MANET. Several routing protocols have been proposed in recent years for deployment of MANET. There are three type sof MANET routing protocols reactive, proactive and hybrid. In this paper we have analyzed all these approaches and discussed their pros and cons. The practical reason behind failure of these approaches is asymmetric link. From analysis we have proposed Novel Approach for Routing in MANET (NARM) which is combination of three approaches reactive, proactive and zone based.

Keywords- Communication Engineering, Wireless Adhoc networks, MANET

I. INTRODUCTION

MANET provides a clear stage making of making} a network in things wherever creating the infrastructure would be not possible or prohibitively high-ticket. Not like a network with fastened infrastructure, mobile nodes in impromptu networks don't communicate through the fastened structures. A billboard hoc network is self-organizing and adaptive. Networks square measure shaped on-the-fly, devices will leave and be part of the network throughout its period, devices are often mobile at intervals the network, the network as a full is also mobile and therefore the network are often unshapely on-the-fly. Wireless devices communicate directly with devices within their radio target a peer-to-peer nature. If they want to speak with a tool outside their vary, they will use associate degree intermediate device or devices at intervals their radio vary to relay or forward communications. Every mobile node acts as a bunch once requesting/providing info from/to alternative nodes within the network, and acts as router once discovering and maintaining routes for alternative nodes within the network.

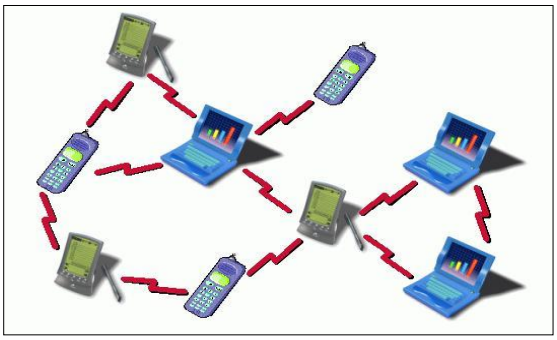

Fig. 1: Fig. 1 Mobile Adhoc Network.

Routing in mobile impromptu networks faces extra issues and challenges compared to routing in ancient wired networks with mounted infrastructure. The routing protocols for Adhoc networks area unit Proactive routing protocol and Reactive routing protocol. The proactive routing protocols area unit Table driven. A routing table is maintained by every node within the network.

The table contains the routing entries for all the doable nodes within the painter. These protocols permit each node to possess a transparent and consistent read of the configuration by propagating periodic updates .Therefore, all nodes area unit able to create immediate choices concerning the forwarding of a selected packet. On the opposite hand, the employment of periodic routing messages has the impact of getting a continuing quantity of communication traffic within the network, completely freelance of the particular information traffic and therefore the topology changes. The reactive routing protocols area unit on demand routing protocols. The routes area unit propagated solely on demand. The information packets transmitted whereas a route discovery is in method area unit buffered and area unit sent once the trail is established. Dynamic supply Routing (DSR) and AODV area unit on demand routing protocols. DSDV could be a table driven routing protocol. These area unit the unremarkably used protocols in MANETs.

The security problems with MANETs area unit more difficult in an exceedingly multicasting setting with multiple senders and receivers. The matter of routing in such environments is aggravated by limiting factors like quickly dynamic topologies, high power consumption, low information measure and high error rates.

II. BLACK HOLE ATTACK

General attack varieties are the threats against Physical, MAC, and network layer that are the foremost necessary layers that operate for the routing mechanism of the circumstantial network. Attacks within the network layer have usually 2 purposes: not forwarding the packets or adding and dynamic some parameters of routing messages like sequence range and hop count. As a consequence, routing in painter has become the most difficult issue as a result of a network with a changeable topology results in frequent path failure. Most accessible routing protocols are classified into 3 types: proactive, reactive and hybrid. beyond question, a painter uses reactive routing protocols, that are additional sensible for such a network owing to the low routing overhead that they turn out and therefore the low power resources that they have.

Recently, many routing protocols are utilized in painter, as well as the AODV protocol [5], Dynamic supply Routing (DSR) [6], Location motor-assisted Routing (LAR) [7] and Zone Routing Protocol (ZRP)[8]. Basically, in routing protocols like AODV and NCPR, once there are knowledge to be sent to a specific destination, the supply node should check its routing table for the destination node if there's any; otherwise, it initiates a supposed RREQ and broadcasts it to any or all nodes. A part attack is one during which a malicious node advertises itself as having the shortest path to a destination during a network. This could cause Denial of Service (DoS) by dropping the received packets. In part attack, the malicious node waits for the neighbors to initiate a RREQ packet. Because the node receives the RREQ packet, it'll instantly send a false RREP packet with a changed higher sequence range. So, that the supply node assumes that node has the recent route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects and data packets

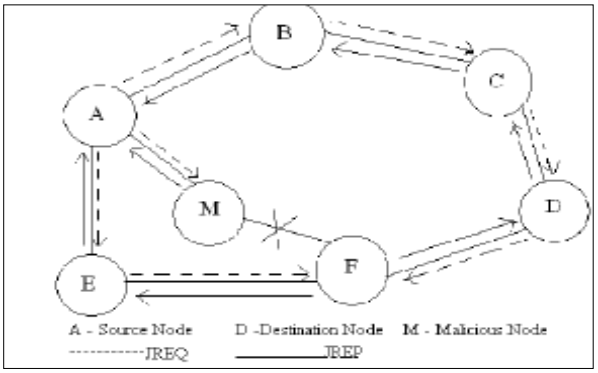

Fig.2 Black Hole Attack

III. PROBLEM STATEMENT

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of mobile nodes. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use.

Solution to the Challenges

We are using different routing protocol to establish a correct and efficient route between a pair of nodes. But because of the limited available power of each node, the selected route cannot remain for a long time so that the source-destination pair can use it for its successful communication. To achieve the goal of getting longer lifetime for a network, we should minimize nodes energy not only during active communication but also when they are in inactive state. Two approaches to minimize the active communication energy are:

1. Transmission power control approach and
2. Load distribution approach and to minimize energy during inactivity [10] the following approach is used

1. Sleep/power-down mode

Transmission Power Control Approach

A routing algorithm essentially involves finding an optimal route on a given network graph where a vertex represents a mobile node and an edge represents a wireless link between two end nodes that are within each other's radio transmission range. When a node's radio transmission power is controllable, their direct communication ranges as well as the number of its immediate neighbours are also adjustable. While stronger transmission power increases the transmission range and reduces the hop count to the destination, weaker transmission power makes the topology sparse which may result in network partitioning and high end-to-end delay due to a larger hop count.

2. Load Distribution Approach

The specific goal of the load distribution approach is to balance the energy usage of all mobile nodes by selecting a route with underutilized nodes rather than the shortest route. This may result in longer routes but packets are routed only through energy-rich intermediate nodes. Protocols based on this approach do not necessarily provide the lowest energy route, but prevent certain nodes from being overloaded, and thus, ensures longer network lifetime. This subsection discusses two such protocols: Localized Energy-Aware Routing (LEAR) and Conditional Max-Min Battery Capacity Routing (CMMBCR) protocols.

IV. LITERATURE SURVEY

Many researchers have addressed the region attack downside in painter. Most of the solutions planned and enforced were supported AODV and DSDV protocol.

Umang singh [1] Mobile Ad hoc Networks are assortment of mobile terminals or nodes, allowing no stationary infrastructure and centralized administration. A performance evaluation of routing protocol is very cumbersome due to various metrics involving dynamic topologies, mobility, routing limited resources, security etc. In this paper, various existing routing protocols were reviewed. It has been analyzed that efficiency of existing routing protocol degrades in the presence of attacks. Keeping in various attacks reports in literature and the protocol security algorithm; this paper attempts to review all such secure routing protocols comparing their relative metric and requirements.

E.A Virgin Mary Anita et al [2] planned an answer enforced on the highest of ODMRP protocol. The authors planned a certificate based mostly authentication mechanism to counter the result of region attack. Nodes evidence one another by provision certificates to neighboring nodes and generating public key while not the requirement of any on-line centralized authority.

Jiwen CAI, Ping YI, Jialin bird genus, Zhiyang WANG, Ning LIU [3] planned associate reconciling approach to find black and grey hole attacks in spontanepous network supported a cross layer style. In network layer, a path-based methodology to take in consequent hop's action. This theme doesn't channelise further management packets and saves the system resources of the sleuthing node. In raincoat layer, a collision rate news system is established to estimate dynamic sleuthing threshold therefore on lower the false positive rate below high network overload. They select DSR protocol to check algorithmic rule and ns-2 as simulation tool.

Wei Gong, Zhiyang You, Danning Chen, Xibin Zhao, Ming Gu, Kwok-Yan Lam [4] planned use of trust vector model based mostly routing protocols. Every node would assess its own trust vector parameters regarding neighbors through watching neighbors' pattern of traffic in network. At identical time, trust dynamics is enclosed in term of lustiness. Then the performance of the planned mechanism by modifying Dynamic supply Routing (DSR) so every node incorporates a dynamic dynamic "trust vector" for its neighbors' behaviors.

N. Bhalaji1, Dr. A. Shanmugam [5] planned associate improvement of the Association based mostly Route choice to be applied to the DSR protocol so as to reinforce its routing security. The aim of applying the association based mostly route choice to the DSR protocol is to fortify the existing implementation by selecting the best and securest route in the network. In contrast to the current route selection in the DSR which involves selection of the shortest route to the destination node, our proposed protocol choose the most reliable and secure route to the destination based on the trust values of all nodes. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes

K.Selvavinayaki K.K.Shyam Shankar Dr.E.Karthikeyan [6] proposed solution that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on DSR protocol and needs to be simulated and analyzed for different performance parameters .This method is capable of detecting and removing black hole nodes in the MANET.

Shilpi Agarwal, Rajeshwar Lal Dua [7] Wireless Sensor Networks (WSNs) are group of small sensor nodes and wireless communication capabilities. The functionalities and parameters of personality strategy in the wireless sensor network (WSN) are very incomplete like processing speed, storage capacity, and communication bandwidth. When these devices are included, it will have processing capabilities, but not individual. The individual devices in a wireless sensor network (WSN) are inherently resource controlled: the network must operate for long periods of time and the nodes are wireless, so the available energy resources whether batteries, energy harvesting, or both limit their overall operation. To minimize energy consumption, most of the device's components, including the radio, will likely be turned off most of the time.

Devendra Prasad and Reema Goyal [8] Wireless Sensor Networks (WSNs) differs from traditional wireless networks in several ways. One of them is energy constraints. Sensor nodes (SNs) are battery operated, with limited life and difficult to replace, if deployed in hostile environment. Therefore protocols in WSNs must be designed with minimum energy consumption to prolong the network life. In WSNs protocols are designed to minimize energy consumption and preserve the longevity of the network. In this paper, we have designed Secure and Energy Efficient Centralized Routing Protocol (SEECH) for hierarchical WSNs. In SEECH, the base station (BS) collects information about the logical structure of the network and residual energy of SN. With these information, BS does efficient clustering. Finally, SEECH is compared with LEACH-C protocol.

Sunita Rani, Er.Tarun Gulati [9] Wireless sensor network is an ad hoc network. Each sensor is defined with limited energy. Wireless sensor node deployed into the network to monitor the physical or environmental condition such as temperature, sound, vibration at different location. Each node collected the information than transmit to the base station. The data is transfer over the network each sensor consume some energy in receiving data, sending data. The

lifetime of the network depend how much energy spent in each transmission. The protocol play important roll, which can minimize the delay while offering high energy efficiency and long span of network lifetime. One of such protocol is PEGASIS, it is based on the chain structure, every chain have only one cluster head, it is in charge with every note's receiving and sending messages who belong to this chain, the cluster head consumes large energy and the times of every round increasing. In PEGASIS, it take the advantage of sending data to it the closet neighbor, it save the battery for WSN and increase the lifetime of the network. The proposed work is about to select the next neighboring node reliably. For this it will combine few parameters such as Distance, Residual Energy and Response time. The proposed system will increase the overall communication and increase the network life.

Nasir Fareed Shah, Shefali Gautam [10] The area of wireless sensor network (WSN) being alluring among community of researchers finding it to be diverse for instance defence security, civilian applications & medical research. Issues of routing in WSN for the sake of usability in computationally constrained and resource constrained micro sensors are complex. Aforementioned coercion hinder line-up of conventional networking system devised for categorical ad-hoc sensor networks. Routing algorithms or protocols being devised for wireless sensor applications need to be candid, and shall upgrade endurance of the Wireless Sensor Network. We proposed a cinch, smart, and adaptive algorithm that assures upgraded endurance of the network.

Hayfa AYADI, Ahmed Zouinkhi, Thierry Val [11] Nowadays the energy consumption has become a critical challenge in Wireless Sensor Network (WSN). Wireless connection suffer from some weaknesse chiefly fault detection and energy efficiency which stay again the main problems in (WSN). Both was under the scope of research communities and industry engineers. We are interested to the IEEE 802.15.4 standard with beacon enabled mode. IEEE802.15.4 is a protocol designed to Physical (PHY) layer and Medium Access Control (MAC) for WSN. We intervene in the Superfame Duration (SD) which present the main private characteristic of the MAC frame in IEEE 802.15.4 in order to minimise the energy consumption when the energy level in a battery reach a critical level. INETMANET/ OMNeT++ simulator is used to present our method.

V. PROBLEM IDENTIFICATION

To perform route discovery, the source node broadcasts a route request packet with a recorded source route listing only itself. Each node that hears the route request forwards the request (if appropriate), adding its own address to the recorded source route in the packet. The route request packet propagates hop-by-hop outward from the source node until either the destination node is found or until another node is found that can supply a route to the target. Nodes forward route requests if they are not the destination node and they are not already listed as a hop in the route. In addition, each node maintains a cache of recently received route requests and does not propagate any copies of a route request packet after the first. Further, when a node receives a route request for which it has a route in its cache, it does not propagate the route request, but instead returns a *route reply* to the source node. The route reply contains the full concatenation of the recorded route from the source, and the cached route leading to the destination.

Ad-hoc on-demand distance vector (AODV) routing protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. AODV routing protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom.

ODV makes sure the route to the destination does not contain a loop and is the shortest path. Route requests (RREQ), route replay (RREP), route errors (RERR) are control messages used for establishing a path to the destination, sent using UDP/IP protocols when the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. When data packets are transmitted between source and destination, due to some security vulnerabilities, some attacks occur and they absorb the data packets by suspending the transmission.

There are several attacks like passive eavesdropping, gray hole attack, black hole attack etc. Here solution to black hole attack is proposed. Every point has some pros and cons. Like this the AODV has some limitations, which makes the annoyance in communication. The weakness of AODV as follows

1. Rush attack with RREQ: this attack means suppress of the valid RREQ sent by a real originator.
2. False message propagation with RREQ: the goal of this attack is reroute the traffic through the malicious node, and then throw it away.
3. False reply with RREP: this attack seizes a request with an answer, before it reaches its destination.

4. False message propagation with RREP: in this attack, the malicious node tries to reroute traffic by using false RREP. The purpose is to abandon the traffic.
Naturally, if a route request packet reaches the destination node, the destination node returns a route reply packet to the source node with the full source to destination path listed.

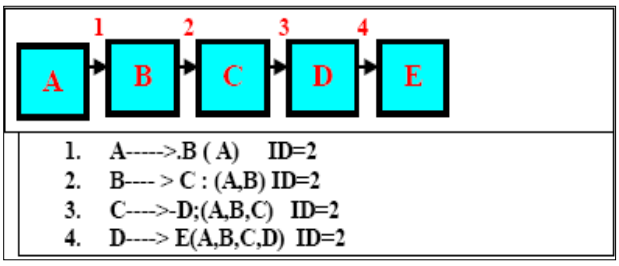

Fig. 3 Route Discovery Process

Route Maintenances is the mechanism by which node **S** is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D. In response to a single Route Discovery (as well as through routing information from other packets overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid. For example, in the situation illustrated in Figure, node A has originated a packet for E using a source route through intermediate nodes B, C and D.

In this case, node A is responsible for receipt of the packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D, and node D is responsible for receipt finally at the destination E.If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet. For example, in Figure 3.2, if C is unable to deliver the packet to the next hop D, then C returns a ROUTE ERROR to A, stating that the link from C to D is currently "broken." For sending such a retransmission or other packets to this same destination E, If A has in its Route Cache another route to E (for example, from additional ROUTE Reply from its earlier Route Discovery, or from having overheard sufficient routing information from other packets), it can send the packet using the new route immediately.

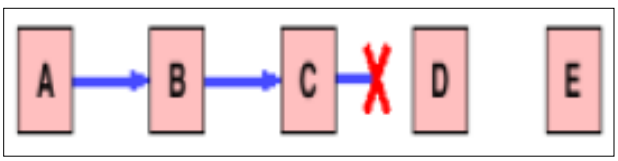

Fig.4 Route Maintenance Process

The existing routing protocols are optimized to perform the routing process without considering the security problem. Adhoc routing protocols is one of the routing attacks in which, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. There is a certificate based authentication mechanism to counter the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority. The proposed scheme is implemented in two phases: certification phase and authentication phase following the route establishment process of On Demand Multicast Routing Protocol (ODMRP) [3].
Following problems are found previous work-
1. Node section approach is very complex.
2. Black hole attack and Jamming is higher hence Packet delivery ration is low.

VI. CONCLUSION

The expected outcome, based on the comparative analysis of MANET routing protocols under different parametric values is the fine categorization of the high-quality of MANET routing protocols with respect to their performance and distinguished environment.
The safety requirements for Ad hoc networks are almost identical for the wired or wireless networks with infrastructure. The security services are based on three concepts: authentication, confidentiality, data integrity and non-repudiation of users.
A. Authentication: The first concept is that authentication controls the identification of a node or entity in the network. Authentication ensures control of access to network resources. With the lack of authentication, malicious nodes can easily assume the identity of another with the aim to attack or take the privileges assigned to that node.
B. Confidentiality: Confidentiality ensures protection of information against threats that may lead to the disclosure of information. Confidentiality ensures private communication between nodes; is based on encryption. Encryption that can be applied to different levels of protocol layers. Encryption algorithms require encryption keys before sending it to the destination. However at the destination one must have the decryption key to decrypt the message.
Applications used
Wireless networks are widely used include cellular phones which are part of everyday wireless networks, allowing easy personal communications. Another example, Inter-continental network systems, use radio satellites to communicate across the world. Emergency services such as the police utilize wireless networks to communicate effectively as well. Individuals and businesses use wireless networks to send and share data rapidly, whether it be in a small office building or across the world.In this proposal for upcoming thesis with theme of analyzing routing protocols in MANET, various explorations along with certain

achievable will be prepared. From brief overview of problem identification to study objectives and scope, multiple motivational and questionable arguments had been identified. Further a detailed discussion investigated the related and interrelated work done in MANET domain with different considerations like mobility and reliability over routing protocols. In methodology, a scalable flow of simulation along with their inputs and outputs and how to analyze results are argued. Finally with simulation design, what to expect and how to make progression through timelines are described. The main contribution of the proposed protocol is to replace the need for preset variables using a novel connectivity metric that provides accurate and precise information about the nodes. Furthermore, the protocol reduces the RREQ routing overhead based on the new dynamic connectivity factor, which significantly improves the overall system performance.

REFERENCES

[1] Umang Singh, "Secure Routing Protocols In Mobile Adhoc Networks-A Survey And Taxanomy" International Journal of Reviews in Computing 30th September 2011. Vol. 7

[2] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET",Journal Of Networks ,Vol.3,No.5,May2008

[3] E. A. Mary Anita and V. Vasudevan, Black Hole attack Prevention in multicast routing Protocols For MANETs Using Certificate Chaining, IJCA, Vol.1, No.12, pp. 22–29,2010

[4] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU , An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network . 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[5] Wei Gong1,2, Zhiyang You1,2, Danning Chen2, Xibin Zhao2, Ming Gu2, Kwok-Yan Lam2,'Trust Based Malicious Nodes Detection in MANET' . 978-1-4244-4589-9/09/$25.00 ©2009 IEEE

[6] N. Bhalaji1, Dr. A. Shanmugam, Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET. JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY, VOL. 2, NO. 2, MAY 2011

[7] K.Selvavinayaki K.K. Shyam Shankar Dr. E.Karthikeyan, Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs . International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 201

[8] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang , Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges . IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION.

[9] Routing Protocols to Enhance Security in MANETS Rakesh Vanaparthiα, Pragati.G Global Journal of Computer Science and Technology Volume 11 Issue 13 Version 1.0 August 2011

[10] K.P.Manikandan, Dr..R.Satyaprasad, Dr. .K.Rajasekhararao "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks" International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011 http://ijacsa.thesai.org/

[11] Santhosh Krishna B.V, Mrs.Vallikannu A.L [12] "Detecting Malicious Nodes for Secure Routing in MANETS Using Reputation Based Mechanism "International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[12] M. Ayyash, Y. Alsbou, and M. Anan, "Introduction to mobile ad-hoc and vehicular networks," in Wireless Sensor and Mobile Ad-Hoc Networks. Springer, 2015, pp. 33–46.

[13] H. Safa, M. Karam, and B. Moussa, "Phaodv: Power aware heterogeneous routing protocol for manets," Journal of Network and Computer Applications, vol. 46, pp. 60–71, 2014.

[14] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in Mobile Computing 99. ACM, 1999, pp. 151–162. [4] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," Wireless networks, vol. 8, no. 2-3, pp. 153–167, 2002.

[15] C. Perkins, E. Belding-Royer, S. Das et al., "Rfc 3561-ad hoc on-demand distance vector (aodv) routing," Internet RFCs, pp. 1–38, 2003.

[16] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPV4, 2007.