Review on Various Mobility Prediction Routing Algorithms for Mobile Ad hoc Networks

Satav Sandip Dattatraya[1]* Dr. Avnish Raj Verma[2]

[1] PhD Student, Maharishi University of Information Technology, Lucknow

[2] PhD Guide, Maharishi University of Information Technology, Lucknow

Abstract – Remote versatile impromptu networks are delineated as networks with no physical associations. In these systems, there is no fixed topology in view of the adaptability of there is no fixed topology due to the adaptability of hubs, obstruction, multipath engendering, and way misfortune. Consequently, a dynamic steering convention is required for these networks to work appropriately. Many Directing conventions have been produced for achieving this undertaking. So as to decide productive, powerful and adaptable steering in MANET, there is a need to build up a directing algorithm that is completely mindful of the present network topology and accessible assets. A multi-objective unicast MANET course improvement issue that utilizations network execution estimates, for example, delay, bounce separate, burden, cost, and dependability are tended to in this examination. In this paper, we exhibited a methodical audit of various investigations of portable specially appointed steering conventions. The examination and comparative analysis of recent studies related to the AODV (Ad-hoc On-demand Distance Vector), DSR (Dynamic Source Routing), ZRP (Zone Routing Protocol), and DSDV (Destination sequenced distance vector). The outcome of this paper claims the various research gaps identified from the literature review.

Keywords - Secure Routing, Mobility Prediction, Mobile Ad Hoc Networks, AODV.

- X -

1. INTRODUCTION

Directing conventions for MANETs have been characterized by the systems of finding and keeping up courses into three classes first is proactive, second is receptive, and final third is hybrid [1]. Evidently, each organizing protocol responds contrastingly to center point adaptability and thickness. A controlling protocol for MANETs is normally assessed as far as execution measurements that are the start to finish delay, overhead, throughput, and information conveyance proportion. This segment diagrams the fundamental highlights of each class. Likewise, a short outline of the protocols that have been utilized in simulations is given.

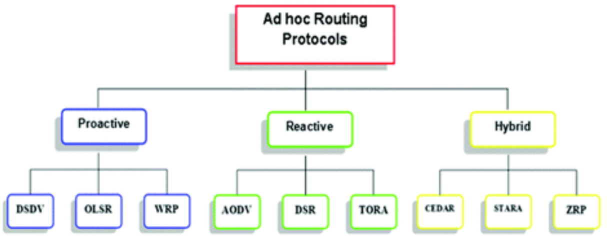


Figure 1: category of routing protocols in MANET

Proactive Routing Protocols: In the first Proactive routing protocols get routing data now and again and store them in at any rate one directing tables. The refinements among the conventions in this class are directing structure, the proportion of tables, and a repeat of invigorates, use of welcome messages and the nearness of a central focal centre point. In this way, every protocol responds diversely to topology variety. Flooding of directing information is the structure that is normally used to discover and used to find and revive courses. In any case, usually proactive protocols produce more control the amount of activity over a communication system during a given period of time and above then another showing classes in perspective on discontinuous reviving which additions as the measure of hubs increments. In addition, tables verifying of high control memory. Points of view proactive controlling conventions are Fisheye State Routing (FSR), and Wireless Routing Protocol (WRP). With WRP [3], every hub keeps up four guiding tables. As the framework gathers, this convention uses a ton of memory. What's more, hello their messages are utilized to guarantee openness with acquaintances. Consequently, this will stuff up more data transmission and control. FSR [4] is a different proactive appearance. This protocol refreshes arrange data every now and again for nodes that are inside its degree as it were. Along these lines, it is more adaptable than WRP. Be that as it may, FSR isn't versatile to greater portability.

Reactive Routing Protocols: Reactive routing protocols get or keep up a sequence as needed. This turns the expenses that are caused by proactive protocols [1, 5]. Flooding methodology is appropriated to find a route. Responsive routing protocols can be classified into two social events: source routing including skip by bounce routing. In source routing, message bunch headers pass on the best approach to deal with an objective. Consequently, transitional nodes couldn't care less about keeping up the routing data. Then again, this sort of protocol may encounter an abnormal state of overhead as the amount of center hubs increases. In like manner, they have a higher shot of a course of disappointment. Parcels in the second gathering of responsive protocols need to convey just goal and next bounce tends to which implies that nodes need to keep up and store routing data for dynamic courses. As a rule, responsive protocols experience the ill effects of postponements on account of the course revelation process. Impromptu On-Request Separation Vector (AODV) [1, 6] and Location Association Routing i.e. LAR, and DSR means Dynamic Source Routing protocol are outstanding receptive routing protocols. AODV is hop routing protocol, which make familiar with a progressively powerful procedure with find and fixes course when contrasted with DSR. Goal succession numbers are utilized to maintain a strategic distance from the issue of unending circles. AODV keeps up just dynamic courses to lessen overheads and control transfer. This show is important for multiple elements of hub thickness, adaptability, and loads. It is reduced for situations with moderate adaptability and density networks. DSR is an active source routing protocol networks. DSR is a responsive source routing protocol [1, 7]. Depreciation and control traffic. This representation is significant for several elements of hub thickness, adaptability, and loads. It is expected for situations with leading adaptability and compactness networks. DSR is a responsive source routing protocol [1, 7]. It obtains establishments on solicitations using field divulgence and foundation system. This convention has two strategies for course disclosure. Right off the bat, it constrains the RREQ spread for characterize territory. Besides, stores the directions of the goal node where the course demand bundles travel toward the goal organizers. This decreases overheads. Be that as it may, every node requirement becomes a GPS.

Hybrid Routing Protocols: Hybrid protocols determine both responsive and proactive highlights. A proactive approach is appropriated to find and Fulfill requirements to attach hubs, while routes to far away hubs are found responsively. In like manner, expenses and allows those are determined by proactive protocols and access protocols, easily, are enforced. Hybrid protocols have been identified to obtain adaptable than many several hubs receive in routing and topology presentation. In Zone Routing Protocol Al Amri, Abolhasan furthermore Wysocki in Methods of the General Assembling at Sign Arranging and Correspondence Frameworks (2007) (ZRP), these hubs are assembled into zones. Changes between hubs relying on their operations in the zone. Another example of a mutt protocol that can adapt to variations in hub diameter and mobility is the Versatile Area Update Routing Protocol (Guzzle). It appropriates GPS data to deal with the hub area and becomes an excuse commonly routing. Every hub is connected with a home locale and sends its new area to its home district as it moves. As such, when a course is needed, the source hub typically requires reviewing the home region of the target. This protocol is suitable for tremendous networks where the measure of hubs and their preferences are high [1, 7]. Hierarchal and Geographic Routing Protocols MANET routing protocols can be separated moreover according to routing structures into level routing protocols, hierarchal routing protocols, and moreover geographic position data supported routing protocols [2, 7]. Each protocol courses message proactively or responsively or utilize the combination of the two strategies. Level protocols can be delayed stimulated like DSDV and on-request protocols (open) like DSR. Those protocols have been described leading of time. The prospect of remote hierarchal routing protocols is to collect adaptable hubs to reduce the zone of flooding. The hubs are obtained with respect to parties, trees or zones where there is a pioneer that makes sense of how to course in its district. Each hub has unmistakable preference depending upon its region inside the get-together or more distant it. This methodology decreases the scope of routing tables and routing information [2]. A case of remote hierarchal routing protocols is the ZRP. The advantages of those protocols are in the diminishing of overheads and improved scaling of huge networks diverged from level routing protocols. In any case, when hub conveyability is high, hierarchal routing may familiarize even more overhead due to gathering re-computation. What's more, a bunch head is a basic node and correspondence separates on the off chance that it goes. Geographic position information supported routing protocols to improve routing by utilizing the Global Position System (GPS) beneficiaries combined with the hubs to get their region information [2]. Those protocols course the data using Geographic Tending to and Routing (GeoCast) where messages are sent to all hubs in unequivocal land regions. GeoCast utilizes topographical data as opposed to intelligent locations. Geological data about nodes takes out the engendering of routing data. Henceforth, geological protocols have greater profitability in acclimating to alteration in hub thickness contrasted with different protocols. Instances of geographic routing are DREAM and Guzzle. Be that as it may, mapping address to area delivers more overheads. What's more, utilizing GPS expends the intensity of a portable node.

Division II performs a literature review of secure and reliable routing applying mobility prediction algorithm for mobile ad hoc networks. Division III performs comparative study and research gaps. Part IV grants the conclusion and future work.

2. LITERATURE REVIEW

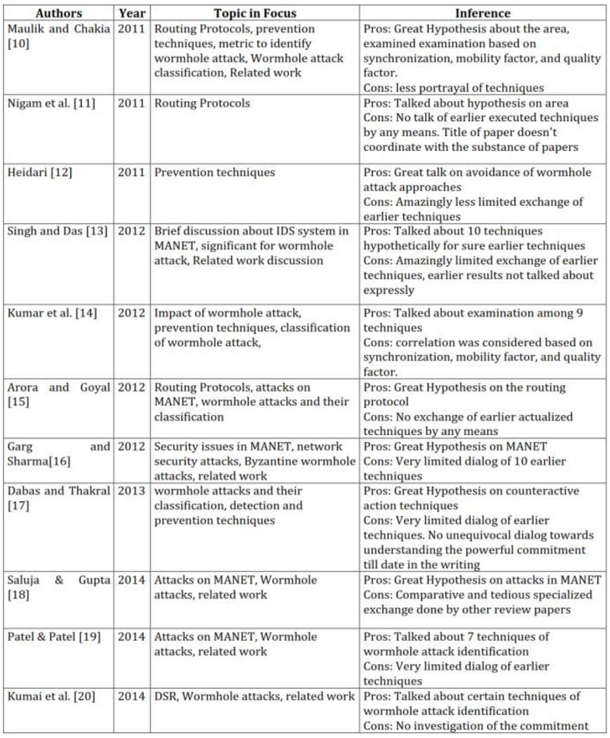
MANET routing protocols stand measures to be tracked by each defeated hub over pleasingly discovers perfect ways and course bundles between endpoints (source and objective hubs). Strong MANET routing protocols strive to create the surviving of the routing approach supporting the closeness of non-routing strategy under the closeness of non - accommodating hub. Siva kumar and Mahalingam (2011) proposed the complete secure routing protocol is APALLS (Ariadne with Pairwise Authentication and Link Layer Signatures), in view of DSR. APALLS is the primary strong routing protocol that is needed to provide a non-repudiable attestation of dynamic attacks. The first DSR protocol is certainly expected that all nodes will submit to the guidelines. The nearness of nodes that don't hold fast to the guidelines, either intentionally, or because of failing, can deleteriously affect the MANET subnet [8].

Shio et. al (2010) proposed protocols that believe that the sensors, each is operated with GPS receivers or utilize some localization method to discover their locations. Geographical and Energy-Aware Routing is an energy-efficient routing protocol anticipated for routing queries to target regions in a sensor field. Synchronization of power saving with routing is a routing protocol also mainly planned for MANETs. But duplicated packets could remain flow of the network, and sensors will obtain duplicated packets. The time suspension for a packet is the time needed to transfer all sensors in a network. Information-Driven Sensor Query heterogeneous Wireless Sensor Network maximizes information gain and reduces recognition latency.

Chen and Wu (2011) proposed a mysterious multipath routing protocol dependent on mystery sharing. The protocol offers area secrecy, personality namelessness, data, and traffic obscurity by using cryptography innovation and secure sharing in the MANET correspondence technique. In the meantime, a hash function is introduced to notice dynamic attacks in the information transmission process. The protocol can productively frustrate different latent attacks and lessen the successful likelihood of dynamic attacks. [9].

This is a significant issue since sensor networks is exceedingly powerless against node bargains in view of the unattended idea of sensor nodes and the need for altering safe hardware. Roy et. al (2012) make the abstract dissemination approach secure against attacks in which haggled hubs contribute false sub-total qualities. Particularly, the lightweight confirmation algorithm by which the base station can decide whether the figured aggregate comprises any false donation. Irrespective of the network size, the per-node conversation overhead is O(1).

3. COMPARATIVE ANALYSIS



Authors	Year	Topic in Focus	Inference
Maulik and Chakia [10]	2011	Routing Protocols, prevention techniques, metric to identify wormhole attack, Wormhole attack classification, Related work	Pros: Great Hypothesis about the area, examined examination based on synchronization, mobility factor, and quality factor. Cons: less portrayal of techniques
Nigam et al. [11]	2011	Routing Protocols	Pros: Talked about hypothesis on area Cons: No talk of earlier executed techniques by any means. Title of paper doesn't coordinate with the substance of papers
Heidari [12]	2011	Prevention techniques	Pros: Great talk on avoidance of wormhole attack approaches Cons: Amazingly less limited exchange of earlier techniques
Singh and Das [13]	2012	Brief discussion about IDS system in MANET, significant for wormhole attack, Related work discussion	Pros: Talked about 10 techniques hypothetically for sure earlier techniques Cons: Amazingly limited exchange of earlier techniques, earlier results not talked about expressly
Kumar et al. [14]	2012	Impact of wormhole attack, prevention techniques, classification of wormhole attack,	Pros: Talked about examination among 9 techniques Cons: correlation was considered based on synchronization, mobility factor, and quality factor.
Arora and Goyal [15]	2012	Routing Protocols, attacks on MANET, wormhole attacks and their classification	Pros: Great Hypothesis on the routing protocol Cons: No exchange of earlier actualized techniques by any means
Garg and Sharma[16]	2012	Security issues in MANET, network security attacks, Byzantine wormhole attacks, related work	Pros: Great Hypothesis on MANET Cons: Very limited dialog of 10 earlier techniques
Dabas and Thakral [17]	2013	wormhole attacks and their classification, detection and prevention techniques	Pros: Great Hypothesis on counteractive action techniques Cons: Very limited dialog of earlier techniques. No unequivocal dialog towards understanding the powerful commitment till date in the writing
Saluja & Gupta [18]	2014	Attacks on MANET, Wormhole attacks, related work	Pros: Great Hypothesis on attacks in MANET Cons: Comparative and tedious specialized exchange done by other review papers
Patel & Patel [19]	2014	Attacks on MANET, Wormhole attacks, related work	Pros: Talked about 7 techniques of wormhole attack identification Cons: Very limited dialog of earlier techniques
Kumai et al. [20]	2014	DSR, Wormhole attacks, related work	Pros: Talked about certain techniques of wormhole attack identification Cons: No investigation of the commitment

The correlation among the three principle sorts of routing protocols is indicated following Table.2.

Table 2. On the basis of Parameters

Parameters	Reactive protocol	Proactive Protocol	Hybrid Protocol
Routing philosophy	Always Flat	Flat or Hierarchical	Always Hierarchical
Routing Schemes	Follows on demand	Table driven Routing schemes	Combination of both Proactive and Reactive.
Routing Overhead	Low overhead	High overhead	Medium overhead
Latency	High because Of flooding	Low because of Routing tables	Similar to Reactive protocols.
Scalability Level	Unsuitable for large networks	Low as compare to Reactive	Continuously Intended for Huge networks

Synopsis of Routing Protocols based on their focal points and impediments is appeared in the accompanying Table 3.

Table 3. Advantages and Disadvantages of Routing Protocols

Protocols	Disadvantages	Advantages
Reactive	Dormancy is expanded in the system.	Overhead is below Since relating to proactive protocol and free of groups.
Proactive	Overhead is High as the contrast with the Receptive Protocol in the system.	Data is constantly available..
Hybrid	Intricacy Increments because of its huge adaptability.	Sensible for gigantic networks when stood out from others.

4. RESEARCH GAPS

From above literature review we noticed the some research gaps in order to design and study review of mobility prediction routing algorithms for mobile ad hoc networks. As indicated by the headway of research in this domain, we listed the research problems.

- Mobile Specially appointed networks have set up their effectiveness in the arrangement for various fields however they are very defenceless against security attacks. The employable idea of impromptu protocols makes it progressively powerless against pantomime, information altering, and refusal administrations.

- The absence of fixed foundation confines the pertinence of some regular security arrangements, for instance, the public key framework it depends on a unified confided in power and the interruption identification framework which required a fixation point to assemble the review information.

- Unreliability of the wireless medium and the dynamic topology because of node portability and disappointment result in successive correspondence disappointment and high postponement for the way reestablishment. The common remote channel significantly affects the presentation of multipath routing. The portable node may move or medium characteristics may alter. In extraordinarily delegated networks, routing tables should by one way or another mirror these adjustments in topology and routing computations must be adjusted. For instance, in a fixed network routing table reviving occurs for every30sec.

- Asymmetric links: The maximum of the wired networks depends upon the symmetric alliances which are persistently arranged. In any state, this isn't a problem with informal networks as the hubs are insignificant and continually arising from changing their circumstances inside the network. For illustration, suppose a MANET(Mobile Ad-hoc Network) wherever hub B gives a mark to hub An at any rate the effects do not appraise anything concerning the occurrence of the connection in the changed course. ?? Routing Overhead: In remote singularly detailed networks, hubs routinely replace their changed course.

- Routing Overhead: In remote remarkably assigned networks, hubs routinely change their zone inside a network. Hence, some musty fields are carried in the routing table which assists unnecessary routing expenses. Interference: This is the difficult issue with adaptable uncommonly distributed networks as routing overhead.

- Interference: This is the troublesome issue with adaptable incredibly assigned networks as associations travel all over depending upon the synchromesh properties, one transmission may intrude with different and a hub may get transmissions of several hubs and can degenerate the total transmission. hub may get transmissions of various hubs and can deteriorate the total transmission.

5. CONCLUSION AND FUTURE EXTENSION

In this paper demonstrates audits on the mobility prediction routing algorithms for mobile ad hoc networks. This greater mobility of nodes in MANETs points to the routing overhead in the route discovery. Several approaches are studied for reducing the routing overhead in such networks. They have their own advantages and disadvantages. In this paper, we have learned about MANETs and examined probably the most significant routing protocols. The comprehension of the fundamental protocols, their points of interest and constraints are basic for understanding the routing system in MANET's. This will help out in growing new protocols for increasingly vigorous situations and for progressively distressing conditions.

In future work, Security is as yet the primary issue in MANET as topology is open and evolving regularly. Attacks are visited in specially appointed networks so they ought to be limited and there are numerous other routing protocols that can be looked at on changed parameters like bundle conveyance proportion and a start to finish dela.

REFERENCES

1. Abolhasan, M., T. Wysocki, and E. Dutkiewciz (2004). A review of routing protocols for mobile ad hoc networks. Elsevier journal of Ad hoc Networks. l2(1): p. 1-22.

2. Xiaoyan, H., X. Kaixin, and M. Gerla (2002). Scalable routing protocols for mobile ad hoc networks. Network, IEEE, 16(4): p. 11-21.

3. Shree, M. and J.J. Garcia-Luna-Aceves (1995). A routing protocol for packet radio networks, in Proceedings of the 1st annual international conference on Mobile computing and networking. 1995, ACM Press: Berkeley, California, United States.

4. Gerla, M. (2002). Fisheye state routing protocol (FSR) for ad hoc network. 2002, IETF Internet Draft 21. Royer, E.M. and T.

Chai-Keong, A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE [see also IEEE Wireless Communications], 1999. 6(2): pp. 46-55.

5. Perkins, C., E. Belding-Royer, and S. Das (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. 2003: RFC Editor.

6. Johnson, D., Y. Hu, and D. Maltz (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. February 2007: RFC Editor.

7. Young-Bae, K. and H.V. Nitin, Location-aided routing (LAR) in mobile ad hoc networks. Wirel. Netw., 2000. 6(4): pp. 307-321.

8. Seung-Chul, M.W. and S. Suresh (2001). Scalable routing protocol for ad hoc networks. Wirel. Netw., 2001. 7(5): pp. 513-529.

9. Sivakumar Kulasekaran and Mahalingam Ramkumar (2011). "APALLS: A Secure MANET Routing Protocol" Mississippi State University USA, January 2011.

10. Chen, S. & Wu, M. (2011). Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. Journal of Systems Engineering and Electronics, 22(3), pp. 519–527. doi:10.3969/j.issn.1004-4132.2011.03.023.

11. Maulik, R., Chaki, N. (2011). A study on wormhole attacks in MANET. International Journal of Computer Information Systems and Industrial Management Applications, pp. 2150-7988.

12. Nigam, N., Saraf, A., Nagar, C. (2011). A Review New Thread Based Wormhole Attack Prevention Mechanism in MANET. International Journal of Electrical, Electronics & Computer Engineering, Vol.1 (1), pp. 84- 87.

13. Heidari, A. & Azad, I. (2011). A Survey of Wormhole Attack and Countermeasures against that in Wireless Ad-hoc Networks. 5th Symposium on Advance in Science & Technology.

14. Singh, M. and Das, R. (2014). A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network. International Journal of Scientific & Engineering Research.

15. Kumar, S., Pahal, V., Garg, S. (2012). Wormhole attack in Mobile Ad Hoc Networks: A Review. IRACST – Engineering Science and Technology: An International Journal, Vol.2, No. 2.

16. Arora, D., Goyal, S. (2012). A Survey of Routing Protocols and Wormhole Attack in Mobile Ad Hoc Networks. International Journal of Research in Engineering and Applied Sciences. Vol. 2, Issue 2.

17. Garg, A. & Sharma, S. (2014). A Study on Wormhole Attack in MANET. International Journal of Scientific Research Engineering & Technology, Vol. 3 Issue 2.

18. Dabas, P. & Thakral, P. (2013). Detection and Prevention of Wormhole Attack in MANET: A Review. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 3, Issue 3.

19. Saluja, B. K. & Gupta, A.K. (2014). A Survey of Different Approaches to Detect Wormhole attack. International Journal of Computer Science and I1nformation Technologies, Vol. 5 (3).

20. Patel, B. N. & Patel, T.S. (2014). A Survey on Detecting Wormhole Attack in Manet. Journal of Engineering Research and Applications, Vol. 4, Issue. 3, pp. 653-656.

21. Kumari, H., Vyas, G., Dhankar, S. (2014). A Survey of Wormhole Detection and Prevention Technique in DSR Protocol. International Journal of Engineering, Management & Sciences, ISSN: 2348 – 3733, Vol. 1, Issue 9.

22. Chaoming Wang; et. al. (2016). “Hybrid Multihop Partition-Based Clustering Routing Protocol for WSNs”, ISSN: 2475-1472, Volume: PP, Issue: 99, pp. 1-1.

23. Jiao wen-cheng, PENG Jing, Zheng, (2010). “Research and Improvement of AODV Protocol in Adhoc Network,” Proc. of 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), IEEE Computer Society, pp. 23–28.

24. Takhellambam Sonamani Singh; et. al. (2016). “Distance Based Multi Single Hop Low Energy Adaptive Clustering Hierarchy (MS LEACH) Routing Protocol in Wireless Sensor Network”, Advanced Computing (IACC), 2016 IEEE 6th International Conference on, pp. 613-617.

Corresponding Author

Satav Sandip Dattatraya*

PhD Student, Maharishi University of Information Technology, Lucknow