A Comparative Study of Routing Protocols for Mobile Ad Hoc Networks

Prachi Pardhi, Revati Vilas Wable

Information Technology, National Institute of Technology Raipur
G.E. Road, Raipur, Chhattisgarh-492010

chinipardhi@gmail.com
reva.wable@gmail.com

Abstract— Several types of Routing Protocols for mobile ad hoc networks have been proposed recently for their application in various areas such as military, government and many other fields. In this paper, we have proposed a comparative study of various routing protocols for mobile ad-hoc networks particularly emphasizing on its security aspect. Furthermore, we have discussed the comparison among existing routing protocols for MANET. Main factor for comparison is routing methodologies and knowledge required to make routing decisions. The comparison is made on the basis of the following factors: integrity, confidentiality, authentication, non-repudiation and availability. Analysis of the secured version of proposed routing method has been done on the basis of the five security requirements and the same has been shown in the comparison tables.

Keywords— MANET, Routing Protocols, AODV, ARIADNE, DSDV, DSR, SEAD, SRP, TORA, ZRP

I. INTRODUCTION

A. MANET

Mobile Ad Hoc Network (MANET) is a group of mobile devices like mobile phones, laptops, sensors or radios that communicate with each other wirelessly by standard Wi-Fi, cellular, local RF network and others. It provides the needed network functionality without an existing fixed structure. A Mobile Ad Hoc Network [1] or spontaneous network is an infrastructure less, self organized and multi-hop network with rapidly changing topology causing the wireless links to be broken and re-established on-the-fly. The main issue is the requirement that the Routing Protocols must be able to respond quickly to the topological changes in the network. Every node in the network must be able to act as a router. The source and destination might have to communicate through intermediate nodes due to limited bandwidth of nodes. Routing [2] in MANETs has been an active area of research and in recent years various numbers of routing protocols have been brought up for resolving the problems of routing [3]. These protocols are mainly classified into classes i.e. Proactive and Reactive. In Reactive or on-demand RPs, the routes are created only when they are needed. The application of this protocol is evident in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV). Wherein Proactive or Table-driven routing protocols [4] the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and Destination Sequenced Distance Vector Protocol (DSDV). All these protocols are a little insecure because attackers can easily retrieve information about the network topology. Here, a centralized firewall is absent due to its distributed nature of the operation for security, host configuration and routing. Mobile nodes are out performed due to lightweight features, less memory and power. First we emphasize on security aspects of MANET Routing Protocols [5] and later we will present classification of the existing protocols, their types and review their characteristics. Also, wireless links generally have lower stability, reliability, efficiency, and capacity as compared to a wired network. The main characteristics are complete lack of centralized control & frequent dynamically varying network. Advanced features of MANET [6] include data rates compatible with multimedia applications global roaming capability, and coordination with other network structures.

Fig. 1: MANET Architecture

Figure 1 shows the architecture of atypical mobile ad hoc network (MANET). In MANET, each node acts as a host and router, which shows its individuality. It is typically a multi hop network [7] that might change randomly or rapidly with time thereby forming unidirectional or bi-directional links.

B. Network Attack and Defiance

Various kinds of attacks compromise the safe communication of information in MANETs, which can be categorized using different criteria. The attacks [8] are generally classified into as passive and active. A Passive Attack does not disrupt the operation of the protocol, but attempts to discover significant knowledge by listening to traffic. Passive attacks involve obtaining vital routing information by searching about the same in the network. Such assaults are generally difficult to recognize and thus, protecting against such assaults [9] is convoluted. Regardless of whether it is absurd to expect to recognize the specific area of a hub, one might have the option to find data about the network topology, utilizing these assaults. An Active Attack, nonetheless, infuses discretionary parcels and attempts to upset the activity of the convention to confine the accessibility, acquire validation, or draw in bundles bound to different hubs. The objective is essentially to draw in all parcels to the aggressor for examination or to debilitate the network [10].

Such attacks can be recognized and the nodes can be identified. To overcome these assaults, routing protocols need to meet the security requirements like confidentiality, availability, integrity, authentication and non-repudiation. To be more precise it should be protected from any kind of information that could be exposed to unintended entities. Figure 2 shows the probable attack types in Mobile Ad Hoc Network (MANET) for example black hole attack, sinkhole, selfish nodes, gray hole attack, passive eavesdropping, jamming, wormhole attack and DoS attack [11]. The routing protocols were introduced to help resolve these attacks and provide a secured network to the user.

Fig. 2: Types of attacks in MANET

Ad hoc networks are tougher when it comes to receiving the packets for other recipients because of the intermediate nodes so they can easily interrupt the information being routed. The kind of assurance that an entity of concern would not be hampered is crucial. It is necessary to ensure that sending and receiving parties can never deny ever sending or receiving any messages. Despite any kind of Denial of Service (DOS) [12] attack an assurance of survivability should be available.

II. ROUTING PROTOCOLS

Mobile ad-hoc networks consist of wireless nodes that communicate with each other by exchanging the information. The path chosen for transferring the information from one node to another node is called routing and the protocols used are called routing protocols [13, 14, 15]. Figure 3 shows the general classification of the various MANET Routing Protocols.

Fig. 3: MANET Routing Protocols

In this section we shall discuss the classification of existing Wireless Ad hoc routing protocols [16], their characteristic features & types. These protocols can be divided into three categories on the basis of the routing information update mechanism i.e. proactive (table driven) or hybrid, reactive (on demand).

A. AODV

Ad hoc On-demand Distance Vector (AODV) is a combination of both DSR and DSDV protocols. It follows the

basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, as well as the use of hop-by-hop routing, sequence numbers, and periodic signals from DSDV [17]. It utilizes destination sequence numbers to guarantee loop opportunity consistently and by staying away from the Bellman Ford "tally-to-vastness" issue offers fast intermingling when the specially appointed organization geography changes. AODV discovers routes just when required and consequently is receptive in nature. The significant weaknesses present in AODV conventions are: Deceptive increment of grouping number and Deceptive abatement of jump check. Zapata applies security expansions to AODV utilizing single direction hash capacities to serve metric fields in Route Request (Route Discovery). He presented Secure-AODV (SAODV) where he proposes utilizing advanced marks to validate non-changeable data in a start to finish way. Hash affixes are utilized to get variable fields, for example, bounce tally. It is an expansion to AODV Routing Protocol [18]. To protect the Route Discovery mechanism of AODV it is used, by providing security features like integrity, authentication and non-repudiation.

B. DSR

Use of source routing is the distinguishing feature of Dynamic Source Routing (DSR). DSR is a reactive protocol i.e. periodic updates are not used. when necessary it computes the routes and then maintains them. Source routing is a routing technique in which the sender of a packet decides the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. There are two basic parts of DSR protocol: route discovery and route maintenance [19]. A cache to store recently discovered paths is maintained by each node. When a node wants to send a packet, it first checks the cache whether there is an entry for that. Assuming indeed, it utilizes that way to communicate the packet. Likewise it connects its source address on the packet. On the off chance that there is no access in the reserve or the passage is lapsed, the sender communicates a course demand packet to every one of its neighbors requesting a way to the destination. Until the route is found, the sender has pauses. At the point when the route demand packet shows up to some other hubs, they check whether they realize the destination inquired. On the off chance that they have route data, they send back a route answer packet to the destination. Else they broadcast a similar route demand packet. When the route is found, the sender will send its necessary packets utilizing the found route just as addition a section in the cache for sometime later. Additionally the hub keeps the age data of the passage to perceive if the cache is new. At the point when any middle hub gets a data packet, it first sees if the packet is shipped off itself. On the off chance that it is the destination, it gets that else it advances the packet utilizing the way appended on the packet.

C. Hybrid Routing Protocols

These protocols try to accommodate various aspects of proactive and reactive routing protocols. They are generally used to provide hierarchical routing; commonly routing can be either flat or hierarchical [20]. Hybrid routing protocols have difficulty how to organize the network according to the parameters of the network. The disadvantage of hybrid routing protocols is that the nodes that have more routing information are maintained by high level topological information, which leads to more memory and power consumption. Some examples of Hybrid Routing Protocols include ZRP, CEDAR and SRP which have been discussed further. In the following section we have presented few of the proposed routing protocols from each class developed for the ad hoc networks to ensure security. Some of the most important protocols and those which dominate recent [21] literature are AODV, DSR, SRP, ZRP, DSDV and TORA.

D. Flat Routing Protocols

In a flat routing, the nodes communicate directly with each other. The problem with this is that it neither scales well nor allows for route aggregation of updates [22]. It can be further classified as proactive and reactive protocols.

- **Proactive Protocols**

Proactive protocols keep learning the topology of the network by communicating topological information among the network nodes. Thus, when needed a route to a destination, such route information is available immediately. In this protocol each node has to maintain a table. These protocols [23] strive and maintain valid routes to all communication mobile nodes all the time. Thus, periodic route updates are shared or exchanged in order to synchronize the tables. A few examples of table driven ad hoc routing protocols include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV), Optimized Link State Routing Protocol (OLSR) and Wireless routing Protocol (WRP).

- **Reactive Protocols**

The main goal of on demand or reactive routing protocols is to minimize the network traffic overhead. These routing protocols are based on some kind of ‘query-reply’ dialog. They do not try to maintain the recent topology of the network. As soon as there is a need, a reactive protocol invokes a procedure to find a route to the destination; such a procedure involves some sort of flooding the network with the route query. A few examples of source initiated ad hoc routing protocols include the Dynamic Source Routing [24] Protocol (DSR), Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), and Temporally-Ordered Routing Algorithm (TORA). No periodic updates are required for these protocols but routing information is only available when needed.

E. DSDV

Destination Sequenced Distance Vector (DSDV) is a hop-by-hop vector routing protocol that updates each node periodically about the routing broadcast. A table driven algorithm which is based on the improvements made to the Bellman-Ford routing mechanism. Here, each node in the network maintains a routing table. Each entry made in this table has a sequence number associated with it that helps in identifying stale entries to prevent the formation of routing loops. Route broadcasts contain the number of hops to reach the destination, the address of the destination, the sequence number of the information received regarding the destination and the new sequence number. As soon as a neighbor device receives the broadcasted routing message along with the current link cost to the device, it compares this value and the corresponding value is stored in its routing table. If changed, it updates the value and re-computes [25] the distance of the route i.e. the link in the routing table. Every node stores the next routing hop for every reachable destination in their routing table. Further we would follow routing tables for each nodes of this network. The updates of routing table in DSDV are distributed by full dump and incremental method. It allows fast reaction to topology changes by declaring immediate route advertisement about the significant changes in routing table. The main advantage DSDV over standard distance vector routing is the addition of a sequence number in each routing table entry as it prevents routing loops caused by updates being applied out of order. Since the routing information may spread along many different paths through the network multi hop wireless transmission may be a common problem.

F. SEAD

Based on the design of Destination Sequenced Distance Vector routing protocol (DSDV) discussed previously we have a proactive routing protocol i.e. Secure Efficient Ad hoc Distance Vector (SEAD). It is a robust protocol against hackers trying to create incorrect routing state in other nodes. In short, it presents a robust data dissemination mechanism which is suitable for safety applications or any other kinds of application. Though it cannot provide a way to prevent an attacker from tampering the next hop or the destination field in route update. This mechanism [26] can adapt the protocol performance in terms of packet delivery ratio to the application’s requirements. SEAD is robust against multiple uncoordinated attackers creating incorrect routing state in any other node despite the active attackers or compromised nodes in the network.

G. SRP

Based on DSR, Papadimitratos proposed a Secure Routing Protocol (SRP) which provides the correct routing information regarding a pair of nodes only if they have prior security association. This protocol has proven robust against a set of attacks that attempt to compromise the route discovery and is therefore applied as an extension of a multitude of existing routing protocols like DSR and ZRP. Here, the source node initiates the route discovery by sending a Route Request (RREQ) packet usually identified by a pair of identifiers, a random query identifier and a query sequence number to the destination. All the replies are sent back strictly through the same route. It combats attacks [27] that could be a potential threat to the route discovery process and guarantees the acquisition of correct topological information. It relies on the availability of a security association (SA) between the source node (S) and the destination node (T) that could be established using a hybrid key distribution based on the public keys of the communicating parties. In case of DSR protocol, SRP requires including a 6-word header containing unique identifiers that tag the discovery process and a message authentication code (MAC) that is computed using a keyed hash algorithm. SRP can only handle Black Hole attacks. Although it cannot prevent Worm Hole attacks.

H. TORA

Temporally Ordered Routing Algorithm (TORA) is a source initiated on demand routing protocol i.e. highly adaptive, loop-free and is distributed based on the concept of link reversal. The primary objective of this protocol is to limit message transmission in the highly dynamic mobile computing environment. It transmits data packets between source and destination nodes of mobile ad hoc network i.e. it exhibits multipath routing capability. It is designed to reduce communication overhead by adapting local topological changes in ad hoc network. Its main feature is the localization of control packets [28] to a set of nodes near the occurrence of a topological change due to route break. Therefore, each node is required to contain its local routing and topology information about its adjacent nodes.

Fig. 4: Route Creation in TORA

Figure 4 represents the route creation in this protocol. TORA contains an unique ID of the node that defines the new reference level, logical time of link failure, reflection indicator bit and a propagation ordering parameter. It tries to develop a separate

directed acyclic graph (DAG) by each node to its particular destination. When a route to a specific destination is required, the source node broadcasts a query packet [29] comprising the address of the destination that propagates via the network till it reaches either the destination or an intermediate node containing the route to the destination.

I. ZRP

Zone Routing Protocol (ZRP) is a hybrid routing protocol for mobile ad hoc networks that attempts to reduce the initial route discovery delay in case of reactive routing, and the control traffic in case of proactive routing by dividing the network [30] into various zones.. It addresses the problems by combining the best properties of both reactive and proactive approaches hence it is classed as a hybrid reactive/proactive routing protocol.

Fig. 5: ZRP Architecture

In Figure 5, the relationship between the components is illustrated. For each zone proactive routing is used while reactive routing is used between these zones. All the route updates are triggered by NDP that notifies Intra-Zone Routing Protocol (IARP) when the neighbor table is updated. Further, the Inter-Zone Routing Protocol (IERP) uses the routing table of IARP to respond to route queries. IERP forwards queries with BRP and uses the routing table of IARP to guide route queries away from the query source. The inter-zone communication [31] used in this protocol uses on-demand routing to reduce all the unnecessary communication. The network is further divided into routing zones according to distances between the mobile nodes. Consider the hop distance as d and node as N . All the nodes within hop distance of at most d from N belong to the routing zone of N . Peripheral nodes of N would therefore be d hops away from N . However, the issue is to determine the size of the zone. The adaptive nature of the Independent Zone Routing enhances the scalability of the ad hoc network.

III. COMPARISON OF PROTOCOLS

Here, we have presented a comparison between some of the existing routing protocols which we have already discussed in the previous section. Table 1 compares proactive, reactive and hybrid protocols on the basis of control traffic, delay, periodic route updates, route availability, routing information, routing philosophy, scalability and storage requirements. The comparison is on the basis of the characteristic properties of routing protocols in high load networks. In high load conditions, DSR throughput is reduced as there is no metric for identifying stale routes.

Thus, it may cause data packets to be dropped. The route updation column shows how the route tables are updated, which nodes send the update messages and how does it influence the routing overhead. It is observed that more periodic the protocols triggered the overhead more. Also the caching overhead changes according to the number of required routing tables and their sizes. The throughput is influenced by factors like routing overhead and queue length. Table 2 compares the reactive protocols which are AODV, DSR and TORA.

Table 1: Comparison between proactive, reactive and hybrid protocols

Parameters	Proactive	Reactive	Hybrid
Control Traffic	High	Low	Lower than other two types
Delay	Low	High	Low for local destinations and high for inter-zone
Periodic Route Updates	Required always	Not required	Used inside each zone
Route Availability	Always available	Computed as per need	Depends on location of destination
Routing Information	Keep stored in table	Doesn't store	Depends on requirement
Routing Philosophy	Mostly flat	Flat	Hierarchical
Scalability	100 nodes	> 100	> 1000
Storage Requirements	Higher	Dependent on no. of routes maintained or needed	Depends on size of each zone or cluster

Table 2: Comparison of reactive routing protocols

Parameters	AODV	DSR	TORA
Caching overhead	Low	High	Medium
Multipath	No	Yes	Yes
Performance Metrics	Speed	Shortness	Speed
Periodic Updation	No	No	No
Route Creation	By source	By source	Locally
Route Updation	Non-periodic	Non-periodic	High routing overhead
Routing overhead	High	High	High
Throughput	High	Low	Low

IV. CONCLUSION

In this paper we have compared the best known protocols used for securing the routing function in mobile ad hoc networks on the basis of various factors as discussed in the previous section. However, there are still many challenges facing Mobile ad hoc networks. Furthermore, we have discussed the comparison among existing routing protocols for MANET on the basis of the following factors: integrity, confidentiality, authentication, non-repudiation and availability. Here, the main factor for comparison was routing methodologies and knowledge required to make routing decisions. Through analysis of these proposals we understood the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. This is why Mobile Ad hoc Networks are becoming more prevalent in the world with increased use of internet.

ACKNOWLEDGMENT

The authors wish to thank all the reviewers, faculty members who helped us throughout and colleagues for their valuable suggestions and comments that help improve the contents of paper.

REFERENCES

- [1] M. N. Alsaim, H. A. Alaqel and S. S. Zaghloul, "A comparative study of MANET routing protocols," The Third International Conference on e-Technologies and Networks for Development (ICeND2014), Beirut, Lebanon, 2014, pp. 178-182, doi: 10.1109/ICeND.2014.6991375.
- [2] D. P. I. I. Ismail and M. H. F. Ja'afar, "Mobile ad hoc network overview," 2007 Asia-Pacific Conference on Applied Electromagnetics, Melaka, Malaysia, 2007, pp. 1-8, doi: 10.1109/APACE.2007.4603864.
- [3] Maria Rita Palattella, Stefano Scanzio, and Sinem Coleri Ergen. 2019. "Ad-Hoc, Mobile, and Wireless Networks." Springer. <https://link.springer.com/book/10.1007/978-3-030-31831-4>.
- [4] Charles E. Perkins, "Ad hoc Networking", Pearson Publication.
- [5] Michael Ngulube, Alex Hinds, Shaoying Zhu, and Hussain Al-Aqrabi. 2013. "A review of routing protocols for mobile ad-hoc NETWORKS (MANET)." https://www.researchgate.net/publication/272911119_A_review_of_routing_protocols_for_mobile_ad-hoc_NETWORKS_MANET.
- [6] G. Mohandas, S. Silas and S. Sam, "Survey on routing protocols on mobile adhoc networks," 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Kottayam, India, 2013, pp. 514-517, doi: 10.1109/iMac4s.2013.6526467.
- [7] M. N. Alsaim, H. A. Alaqel and S. S. Zaghloul, "A comparative study of MANET routing protocols," The Third International Conference on e-Technologies and Networks for Development (ICeND2014), Beirut, Lebanon, 2014, pp. 178-182, doi: 10.1109/ICeND.2014.6991375.
- [8] Nur Amirah Mohd Saudi, Mohamad Asrol Arshad, Alya Geogiana Bujia, Ahmad Firdaus Ahmad Fadzil, and Raihana Md Saidi. 2019. "Mobile Ad-Hoc Network (MANET) Routing Protocols." Springer. https://link.springer.com/chapter/10.1007/978-981-13-7279-7_7#~:text=In%20this%20paper%2C%20the%20performance,AOMDV%20are%20assessed%20for%20comparison
- [9] M. Karthiga, L. Latha and K. Sriprayan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 396-402, doi: 10.1109/ICICT48043.2020.9112588.
- [10] Saleh Alomari, and Sumari Putra. 2010. "An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications." Research Gate. https://www.researchgate.net/publication/220487867_An_Overview_of_Mobile_Ad_Hoc_Networks_for_the_Existing_Protocols_and_Applications.
- [11] Patroklos Argyroudis, and Donal O'Mahony. 2006. "Secure routing for mobile ad hoc networks." Springer. https://www.researchgate.net/publication/3454648_Secure_routing_for_mobile_ad_hoc_networks.
- [12] Anuj Kumar Gupta. 2009. "Secure Routing Techniques for Mobile Ad Hoc Networks." Research Gate. https://www.researchgate.net/publication/216289181_Secure_Routing_Techniques_for_Mobile_Ad_Hoc_Networks.
- [13] Jaspal Kumar, M. Kulkarni, and Daya Gupta. n.d. "International Journal of Computer Network and Information Security(IJCNIS)."
- [14] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. 2005. "A Secure On-Demand Routing Protocol for Ad Hoc Networks." Springer. <https://link.springer.com/article/10.1007/s11276-004-4744-y>.
- [15] Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose, and Himadri Nath Saha. 2011. "Different types of attacks in Mobile ADHOC Network Different types of attacks in Mobile ADHOC Network." Research Gate. https://www.researchgate.net/publication/51956520_Different_types_of_attacks_in_Mobile_ADHOC_Network.
- [16] G. Kaur and P. Thakur, "Routing Protocols in MANET: An Overview," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT), Kannur, India, 2019, pp. 935-941, doi: 10.1109/ICICT46008.2019.8993294.
- [17] "Ad hoc On-Demand Distance Vector (AODV) Routing." n.d. RFC 3561. <https://tools.ietf.org/pdf/rfc3561.pdf>.
- [18] Anuj K. Gupta, Dr. Harsh Sadawarti, and Dr. Anil K. Verma. 2010. "Performance analysis of AODV, DSR & TORA Routing Protocols." <http://www.ijetch.org/papers/125--T203.pdf>.
- [19] Natarajan Meghanathan. 2010. "Design of a Reliability-based Source Routing Protocol for Wireless Mobile Ad Hoc Networks." Springer.
- [20] A. A. Pirezada, C. McDonald and A. Datta, "Performance comparison of trust-based reactive routing protocols," in IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 695-710, June 2006, doi: 10.1109/TMC.2006.83.
- [21] Asad Amir Pirezada, Amitava Datta, and Chris McDonald. n.d. "Performance comparison of trust-based reactive routing protocols." Research Gate. https://www.researchgate.net/publication/3436512_Performance_comparison_of_trust-based_reactive_routing_protocols.
- [22] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile Ad Hoc routing protocols," in IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 78-93, Fourth Quarter 2008, doi: 10.1109/SURV.2008.080407.
- [23] Manel Guerrero Zapata, and N. Asokan. 2002. "Securing ad hoc routing protocols." <https://dl.acm.org/doi/abs/10.1145/570681.570682>.
- [24] Yih-Chun Hu, and David B. Johnson. 2004. "Securing quality-of-service route discovery in on-demand routing for ad hoc networks." Research Gate. https://www.researchgate.net/publication/220829451_Securing_quality-of-service_route_discovery_in_on-demand_routing_for_ad_hoc_networks.
- [25] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers," August 1994.
- [26] Dr. Anuj Gupta Dr. Anuj Gupta. 2011. "A Review of Routing Protocols for Mobile Ad Hoc Networks." Academia.
- [27] Waleed S. Alnumay, and Uttam Ghosh. 2014. "Secure Routing and Data Transmission in Mobile Ad Hoc Networks." <https://arxiv.org/ftp/arxiv/papers/1402/1402.2108.pdf>.
- [28] "Performance Comparison and Analysis of Preemptive-DSR and TORA." 2010. <https://arxiv.org/ftp/arxiv/papers/1101/1101.0209.pdf>.
- [29] "Security Analysis of TORA Routing Protocol." 2007. Springer. https://link.springer.com/chapter/10.1007/978-3-540-74477-1_87.
- [30] Prince Samar, Marc R. Pearlman, and Zygmunt J. Haas,. 2004. "Independent Zone Routing: An Adaptive Hybrid Routing Framework for Ad Hoc Wireless Networks." <https://people.ece.cornell.edu/haas/Publications/ToN-samar-pearlman-haas-2004-08.pdf>.
- [31] Indra Gupta, Balasubramanian Raman, and Nidhi S Kulkarni. 2009. "On Demand Routing Protocols for Mobile Ad Hoc Networks: A Review." Research Gate. https://www.researchgate.net/publication/224398630_On_Demand_Routing_Protocols_for_Mobile_Ad_Hoc_Networks_A_Review.