Performance Evaluation of QOS Parameters of Hybrid ACO/PSO for Mobile ADHOC Networks

Meenu Punj
Deptt of Computer Science Engg
ACET, Amritsar

Tanupreet Singh
Deptt of Electronics and Communication
ACET, Amritsar

ABSTRACT

The multicast describes the distribution of structures from just one single node to number of destinations. These real-time services have a stringent necessity of QoS factors like bandwidth, delay, jitter etc. to ensure clean, consistent, and fair sign to the receivers. In this paper, in the proposed technique the issue of multi-cast tree has been removed using clustering based technique. First of all multi-radio and multichannel based cluster has been deployed and these cluster head are responsible for the multicasting which decrease the overall energy consumption of nodes and complexity of intelligent algorithms. The path has been evaluated based upon the ant colony optimization. Thus it improves the overall performance of the QoS parameters of Ad-hoc networks.

Keywords: - MANETs, QoS, Jitter, ACO, PSO

1. INTRODUCTION

A portable ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a fresh art of network establishment and could be perfect for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. The most popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this instance, the nodes are limited by send and receive information but do not route anything throughout the network.

Mobile ad-hoc networks can operate in a standalone fashion or may be attached to a bigger network including the Internet. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples add a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we would ever guess several peoples with laptops, in a business meeting at a location where no network services is present. They are able to easily network their machines by forming an ad-hoc network. That is one of the numerous examples where these networks may possibly be used.

2. CHARACTERSTICS OF MANETS

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), Omni directional (broadcast), probably steer able, or some combination thereof [1]. At certain stage, based on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, an instant connectivity in the form of a random, multihop graph or "ad hoc" network exists on the list of nodes. This ad hoc topology may modify as time passes whilst the nodes move or adjust their transmission and reception parameters.

The characteristics of the networks are summarized the following:

a) Communication via wireless means

b) Nodes can perform the roles of both hosts and routers

c) Bandwidth-constrained, variable capacity links

d) Energy-constrained Operation

e) Limited Physical Security

f) Dynamic network topology

g) Frequent routing updates

Advantages of MANETs

Some of the applications of MANETs are the following:

a) Military or police exercises.

b) Disaster relief operations.

c) Mine cite operations.

d) Urgent Business meetings.

3. PROBLEMS IN ROUTING WITH MANETS

i). Asymmetric links: All the wired networks depend on the symmetric links which are always fixed. But this is simply not a case with ad-hoc networks whilst the nodes are mobile and constantly changing their position within network

ii). Routing Overhead: In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table that leads to unnecessary routing overhead.

iii). Interference: Here is the major trouble with mobile ad-hoc networks as links come and go with regards to the transmission characteristics, one transmission might restrict another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

iv). Dynamic Topology: Since the topology isn't constant; therefore the mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. Like in a fixed network routing table updating takes place for every single 30sec. This updating frequency may be very low for ad-hoc networks.

4. LITERATURE SURVEY

D.Zheng et al. [1] proposed a game title theoretic way of quantitatively analyze the attack strategies of the attacker so as to make rational decision on relay selection and the authentication parameter adaptation to reach the trade-off between security and Quality of Service (QoS) in CO-MANETs. Simulation results had shown the effectiveness of the proposed approach for security and QoS co-design in CO-MANETs. Cooperative communication has been proposed to form a virtual MIMO system through strategic relay selection to boost communication quality in wireless networks, including mobile ad hoc networks (MANETs). Due to their unorganized and decentralized infrastructure, MANETs with cooperative communications (CO-MANETs) were at risk of attacks initiated on relays. Although encryption and authentication protocols may prevent compromised data transmission whenever a selected relay has attacked, their cost was high. P.C.Tsou et al. [2] proposed a DSR based secure routing protocol named BDSR (Baited-Black-hole DSR). The BDSR detected and avoids the black hole attack centered on merging proactive and reactive defense architecture in MANET using the virtual and non-existent destination address to bait the malicious node to reply RREP. Due to its easy deployment features, in addition to utilized in personal area networks, home area networks and so on. Specially, MANETs suit for military operations and the emergent disasters rescue that want to overcome terrain and special purpose in urgent. Nevertheless the dynamical network topology of MANETs, infrastructure-less property and lack of certificate authority make the security problems of MANETs need to pay more attention. S.Wong et al. [3] formulated a story graph optimization problem, called Minimal Gateway Assignment Problem, and proved so it was NP-hard. Nonetheless, they provided efficient algorithms to fix this issue with varying quantities of complexity and coordination. First, they provided a centralized polynomial-time algorithm that is 2-approximable, and a distributed algorithm. Second, by simulation, they revealed that their centralized and distributed algorithms could perform near the optimal. They also reported an appealing result that cooperation has been the key factor to create optimal outcomes - an easy algorithm with tight cooperation among MANETs gave far better outcomes than the usual smart algorithm with loose cooperation. I.K.Tabash et al. [4] proposed a fuzzy inference system based on the factors of expected throughput and actual throughput to dynamically adjust the congestion window size that cause improvement in the performance of TCP in MANETs. This proposed scheme didn't count on any explicit feedback from the network; it required only the sender side modifications. The simulation study of the ad hoc network in this work was pertaining to equal sharing of network bandwidth among multiple TCP flows. Through extensive simulations, the authors had shown that how many concurrent flows significantly affect the TCP performance. The proposed scheme achieved the specified goals of improved performance compared to other TCP variants. A.Kumar et al. [5] proposed conceptually a new protocol for MANETs for minimizing maintenance overhead and consequently improving the performance. MANETs consist of nodes which can act as a hub along with host. With the advancement in movement of nodes the configuration of network keeps on changing. This initiates new issues in the dynamically changing scenario of routes and you have to devise for effective mechanisms and deployment for determining new routes in the network. Many routing protocols have been devised adhering to their perspective point of view. R. Song et al. [6] proposed a link layer anonymous access protocol (LAA) to be able to provide strong security and anonymity protection for tactical MANETs. The protocol used dynamic pseudonyms as network and node identities for network access authentication to avoid tracking, tracing, and other common attacks. It used a localized key management mechanism for local shared key and broadcast key establishment that outperformed the connectivity and efficiency of key management in RSN and other link layer security technologies such as for example SEAMAN. Simulations revealed that LAA had merely a small effect on end-to-end delay and no effect on packet delivery ratio in accordance with the conventional MAC, meanwhile providing anonymous communication, better protection and improved connectivity performance in the hyperlink layer for tactical MANETs. N.M. Chacko et al. [7] outlined several routing algorithms in MANETs. Mobile AdHoc Networks (MANETs) includes a wide selection of applications, which range from everyday cell phone application to mission critical military applications. MANETs have proved their necessity and the simple setting up networks. Thus MANETs are extremely popular for scenarios which are sensitive and urgent like disaster relief, military applications, etc. As the application form of MANETs increases, the attacks on MANETs also increase. A vast range of research has been conducted to keep routing in MANETs robust and secure. Among the major research area is routing privacy. Many routing solutions were proposed to keep up privacy. Location aided routing has a book idea; in which routing was done based on location information, therefore node identity was not revealed. J.Gao et al. [8] demonstrated the potential application of the Quasi-Birth-and-Death process (QBD) theory in MANETs delay analysis by making use of it to the end-to-end delay modeling in broadcast-based two-hop relay MANETs. They first demonstrated that the QBD theory actually enabled a book and powerful theoretical framework to be developed to efficiently capture the complicated network state transitions in the concerned MANETs. They revealed that with the help of the theoretical framework, they were able to analytically model the actual expected end-to-end delay and also the actual per node throughput capacity in such MANETs. Extensive simulations were further provided to validate the efficiency of their QBD theory-based models. P. Zhao et al. [9] described that power heterogeneity has been common in mobile ad hoc networks (MANETs). With high-power nodes, MANETs can improve network scalability, connectivity, and broadcasting robustness. However, the throughput of power heterogeneous MANETs may be severely impacted by high-power nodes. To address this matter, they presented a loose-virtual-clustering-based (LVC) routing protocol for power heterogeneous (LRPH) MANETs. To explore the benefits of high-power nodes, they developed an LVC algorithm to construct a hierarchical network and to get rid of unidirectional links. To reduce the interference raised by high-power nodes, they developed routing algorithms to prevent packet forwarding via high-power nodes. Via the mix of analytical modeling, simulations, and real-world experiments, they demonstrated the potency of LRPH on improving the performance of power heterogeneous MANETs. Y.Chen et al. [10] studied the actual throughput capacity under a far more realistic and practical network model for MANETs, where network nodes randomly relocate a continuous unit square without cell-partition and a slotted ALOHA protocol has been adopted for medium access control. For the considered ALOHA MANETs (A-MANETs), they first determined its exact throughput capacity on the basis of the successful transmission probability (STP) and also derived the expected end-to-end delay for a capacity achieving routing algorithm. Then they developed efficient closed-form approximations to both the STP and the actual throughput capacity in the concerned A-MANET under a popular local transmission scheme, based on that your corresponding capacity optimization issue has been explored. Finally, simulation and numerical results were provided to validate the efficiency of their capacity model and to illustrate their theoretical findings. M. Gharib et al. [11] proposed a new probabilistic key management algorithm for large-scale MANETs. To the best of these knowledge, this is the very first method which probabilistically used asymmetric cryptography to control the keys in MANETs. In this algorithm, they stored only some keys in each node rather than all. They analytically proved that the network will remain linked to a higher probability more than 99:99%. Furthermore, they analytically calculated the average path length in the network and showed that this parameter would not have an important increment employing their algorithm. All analytical results were also validated by simulation to create them dependable. W.Liu et al. [12] proposed a generalized i.i.d. mobility model, in which each node moves once after each and every time slots, and remained static between two moves. To investigate the TD trade-off beneath the g.i.i.d. model, they developed a book multi-relay multi-hop (MRMH) scheme that exploited the opportunities of multi-hop transmissions once the network has been static. Furthermore, allow the multi-hop transmissions, they constructed a new percolation highway system that has not been utilized in the TD trade-off analysis for MANETs. Using the proposed MRMH scheme, they developed and proved constructive bounds for throughput and delay in MANETs with various scales of f. Their constructive bound was asymptotically optimal for f = 1. H. Dahshan et al. [13] proposed a trust based threshold cryptography revocation scheme for MANETs. Within their proposed scheme, the master private key was to split into n pieces in accordance with a random polynomial. Each node in the proposed scheme was configured with a before joining the network. Meanwhile, the master private key could be recovered by combining any threshold t pieces predicated on Lagrange interpolation. Consequently, the proposed scheme improved the safety levels in MANETs. The proposed hop-by-hop certificate revocation scheme was predicated on both threshold cryptography and transitive trust between mobile nodes. Due to the decentralized nature of these proposed schemes, it enabled a group of legitimate nodes to do fast revocation of a nearby misbehaving node. The proposed scheme was highly robust in the mobility environment of MANETs. The benefits of the proposed scheme were justified through extensive simulations. S.Tan et al. [14] proposed a mechanism that provided Secure Route Discovery for the AODV protocol (SRD-AODV) in order to prevent black hole attacks. This mechanism required the foundation node and the destination node to verify the sequence numbers in the Route Request (RREQ) and Route Reply (RREP) messages, respectively, predicated on defined thresholds before establishing a connection with a destination node for sending the data. The simulation results using the Network Simulator 2 (NS2) demonstrated an improvement in the ratio of packet delivery for three different environments employing their mechanism as set alongside the standard AODV protocol. A dark hole attack is one kind of malicious attack that can be easily employed against data routing in MANETs. A dark hole node replies to route requests rapidly with the shortest path and the greatest destination sequence number. The black hole node does not need an active route to a specified destination related to it and it drops most of the data packets so it receives. S.Chadli et al. [17] made an intensive analysis of existing attacks. Because of this they proposed a new system to classify attacks predicated on attributes that be seemingly the best classification criteria to generate test-cases. They also applied the classification tree method (CTM) to choose test-cases to attack. Finally, they used the CTE (Classification Tree Editor) tool to generate and select test-cases. Because of the flexibility given by their dynamic infrastructure MANETs were vulnerable to various kinds of security attacks. Furthermore, many conventional security solutions have been developed. However, these proposals suffered from the difficulties of tests and evaluations. Among these solutions the intrusion detection systems (IDS). To improve the quality of protection of MANETs given by intrusion detection systems (IDS), they provided assessment of detection and test procedures far better.

5. PROPOSED METHODOLGY

Figure 1 represents the flowchart of the proposed algorithm.

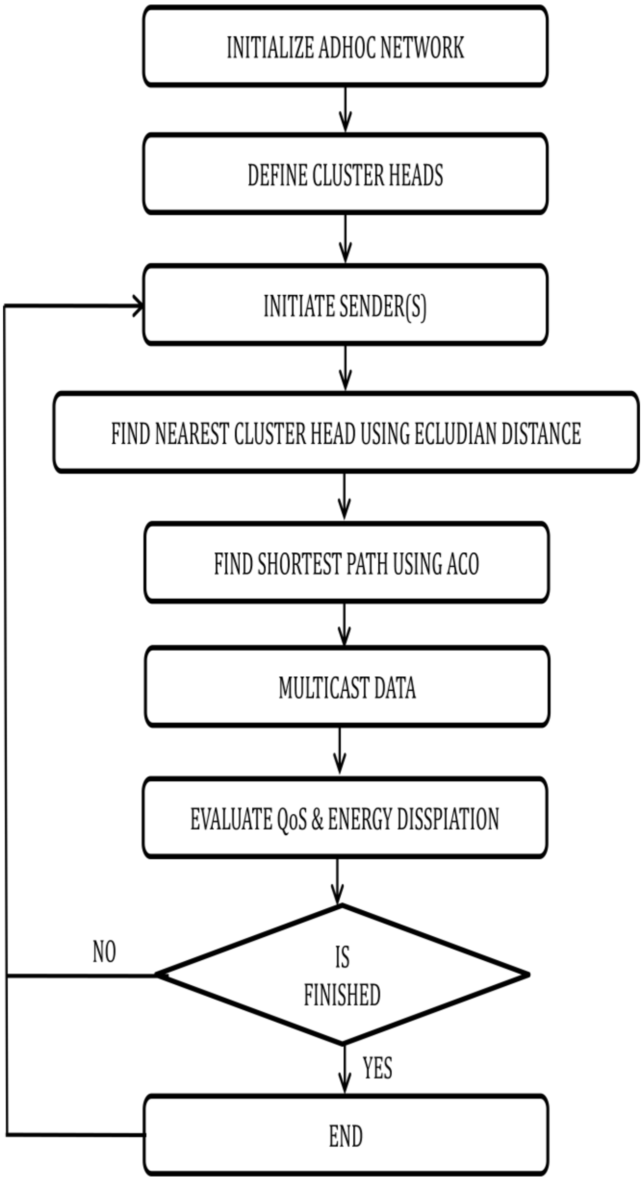
INITIALIZE ADHOC NETWORK
DEFINE CLUSTER HEADS
INITIATE SENDER(S)
FIND NEAREST CLUSTER HEAD USING ECLUDIAN DISTANCE
FIND SHORTEST PATH USING ACO
MULTICAST DATA
EVALUATE QoS & ENERGY DISSPIATION
IS FINISHED
NO
YES
END

Fig 1: Flowchart of the proposed algorithm.

6. RESULTS AND DISCUSSIONS

This section consists of comparison in existing and proposed technique. Table 1 represents the values for various parameters like delay jitter, delay, execution time and tree cost for different experiments.

Table 1: Results of performance metrics

Exp.	Results for Existing Technique				Results for Proposed Technique			
	Delay Jitter	Delay	Execution Time	Tree Cost	Delay Jitter	Delay	Execution Time	Tree Cost
1	115.6000	41.8000	0.1059	22.1294	85.3014	7.5000	0.0039	2.1322
2	97	34.8333	0.1010	21.1177	33.3498	5.5000	0.0034	0.8335
3	89.8571	31	0.1200	26.0428	46.1311	5.5000	0.0118	1.1529
4	72.5000	25.5000	0.0999	20.3835	38.0567	6	0.0034	0.9511

Below are the graphs for different parameters.

Delay jitter: - The term jitter is often used as a measure of the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. However, for this use, the term is imprecise. Or in other word jitter is the variation of the packet arrival time. In jitter calculation the variation in the packet arrival time is expected to minimum. The delays between the different packets need to be low if we want better performance in Mobile Ad-hoc Networks. Fig 2 represents that delay jitter of proposed technique is less as compared to existing technique. Therefore, proposed work outperforms the existing technique.

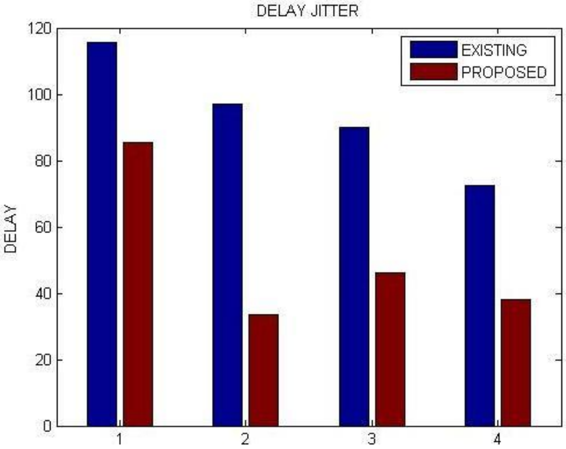

Fig 2: Delay Jitter Analysis

Delay: - The delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. Fig 3 represents that delay of proposed technique is less as compared to existing technique. Therefore, proposed work outperforms the existing technique.

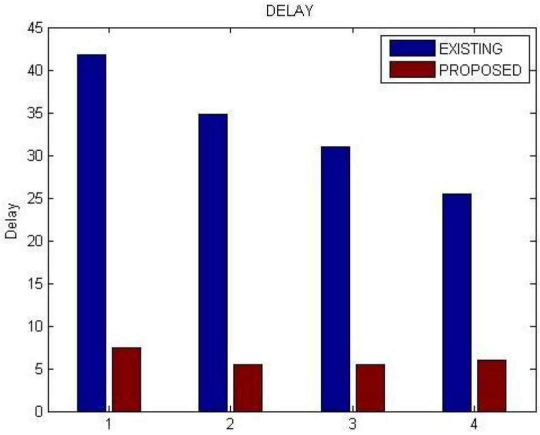

Fig 3: Delay Analysis

Execution Time: - In Mobile ad hoc network (MANET) consist of mobile hosts without any infrastructure. Here the Execution time is the essential parameter in performance analysis for the research peoples. Execution time is the time for executing a particular scenario. Fig 4 represents that execution time of proposed technique is less as compared to existing technique. Therefore, proposed work outperforms the existing technique.

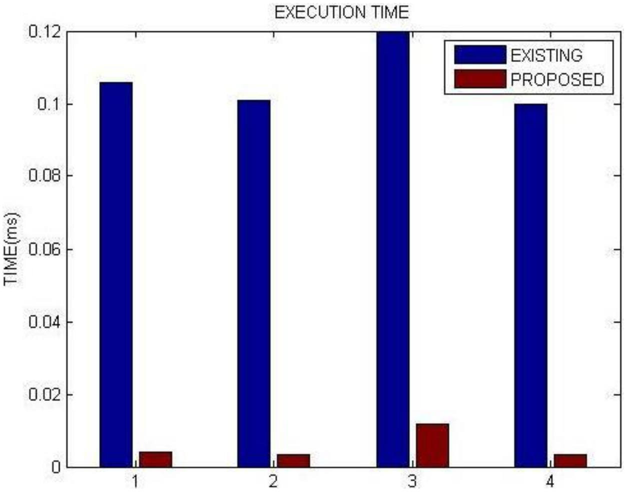

Fig 4: Execution Analysis

Tree Cost: - The total cost of the tree is defined as sum of the cost of all links in that tree. Fig 5 represents that tree cost of proposed technique is less as compared to existing technique. Therefore, proposed work outperforms the existing technique.

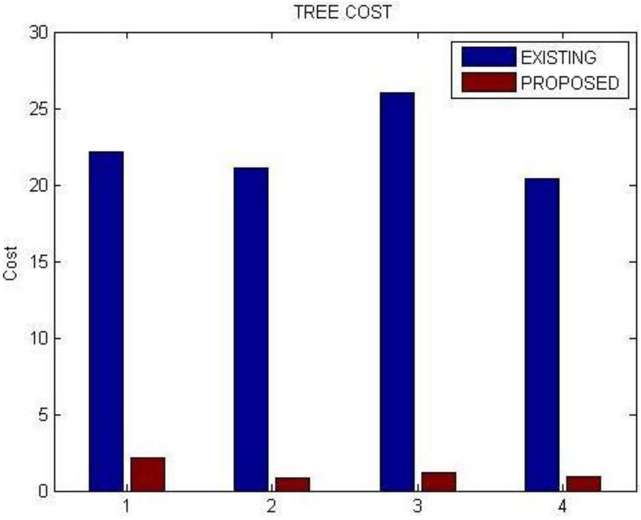

Fig 5: Tree Cost Analysis

7. CONCLUSION AND FUTURE SCOPE

In this paper, a new clustering and ACO based routing algorithm for Ad-hoc networks has been proposed. The proposed technique overcomes the constraints of the earlier work. The main problem of QoS routing is to setup a multicast hierarchy that may meet particular QoS constraint. Nevertheless, the situation of making a multicast tree below numerous constraints is available to be NP Complete. Therefore, the issue is often settled by heuristics or smart optimization. The design and implementation has been done in MATLAB. The performance metrics shows the better performance of proposed algorithm over existing ones. This work has not consider any kind of attacks while transmitting the data, but security is essential component of the adhoc networks so in near future we will propose a new fuzzy based technique which has also the ability to handle attacks.

8. REFERENCES

[1] Zheng, Du. "A Game Theoretic Approach for Security and Quality of Service (QoS) Co-Design in Cooperative Wireless Communication Networks." PhD diss., Carleton University, 2011.

[2] Tsou, Po-Chun, Jian-Ming Chang, Yi-Hsuan Lin, Han-Chieh Chao, and Jiann-Liang Chen. "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs." In *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, pp. 755-760. IEEE, 2011.

[3] Wong, Starsky HY, Chi-Kin Chau, and Kang-Won Lee. "Managing interoperation in multi-organization MANETs by dynamic gateway assignment." In *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, pp. 129-136. IEEE, 2011.

[4] Tabash, Ibrahim K., Nesar Ahmad, and Salim Beg. "A Congestion Window Control mechanism based on Fuzzy Logic to improve TCP performance in MANETs." In *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on*, pp. 21-26. IEEE, 2011.

[5] Kumar, A., S. S. Srivastava, B. Ram, and P. Singh. "Exploring a new dimension in MANETs through a new routing protocol." In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, vol. 5, pp. 328-331. IEEE, 2011.

[6] Song, Ronggong, and H. Tang. "LAA: Link-layer anonymous access for tactical MANETs." In *2012 MILITARY COMMUNICATIONS CONFERENCE, Orlando*, pp. 1-7. 2012.

[7] Chacko, Namrata Marium, Shini Sam, and P. Getzi Jeba Leelipushpam. "A survey on various privacy and security features adopted in MANETs routing Protocol." In *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*, pp. 508-513. IEEE, 2013.

[8] Gao, Juntao, and Xiaohong Jiang. "Delay modeling for broadcast-based two-hop relay manets." In *Modeling & Optimization in Mobile, Ad Hoc & Wireless Networks (WiOpt), 2013 11th International Symposium on*, pp. 357-363. IEEE, 2013.

[9] Zhao, Peng, Xinyu Yang, Wei Yu, and Xinwen Fu. "A Loose-Virtual-Clustering-Based Routing for Power Heterogeneous MANETs." *IEEE transactions on vehicular technology* 62, no. 5 (2013): 2290-2302.

[10] Chen, Yin, Yulong Shen, Xiaohong Jiang, and Jie Li. "Throughput capacity of ALOHA MANETs." In *Communications in China-Workshops (CIC/ICCC), 2013 IEEE/CIC International Conference on*, pp. 71-75. IEEE, 2013.

[11] Gharib, Mohammed, Ehsan Emamjomeh-Zadeh, Ashkan Norouzi-Fard, and Ali Movaghar. "A novel probabilistic key management algorithm for large-scale manets." In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 349-356. IEEE, 2013.

[12] Liu, Wang, Kejie Lu, Jianping Wang, Yi Qian, Liusheng Huang, Jun Liu, and Dapeng Oliver Wu. "On the throughput-delay trade-off in large-scale MANETs with a generalized iid mobility model." In *INFOCOM, 2013 Proceedings IEEE*, pp. 1321-1329. IEEE, 2013.

[13] Dahshan, Hisham, Fatma Elsayed, Alaa Rohiem, Aly Elgmoghazy, and James Irvine. "A Trust Based Threshold Revocation Scheme for MANETs." In *Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th*, pp. 1-5. IEEE, 2013.

[14] Tan, Seryvuth, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." In *ICT Convergence (ICTC), 2013 International Conference on*, pp. 1027-1032. IEEE, 2013.

[15] Mohammad, S. N., M. J. Ashraf, S. Wasiq, S. Iqbal, and Nadeem Javaid. "Analysis and Modeling of Network Connectivity in Routing Protocols for MANETs and VANETs." In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on*, pp. 528-533. IEEE, 2013.

[16] Chen, Kang, Haiying Shen, and Haibo Zhang. "Leveraging social networks for p2p content-based file sharing in disconnected manets." *Mobile Computing, IEEE Transactions on* 13, no. 2 (2014): 235-249.

[17] Chadli, Sara, Mohammed Saber, and Abdelhak Ziyyat. "Defining Categories to Select Representative Attack Test-Cases in MANETs." In *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*, pp. 658-663. IEEE, 2014.