# DYNAMIC & SMART PATH SELECTION MECHANISM FOR CONGESTION AVOIDANCE ON IOT NETWORKS

**[1]Dimple Sharma, [2]Preeti Bansal**
[1]Student, [2]Assistance Professor
Electronics And Communication
Chandigarh Engineering College, Mohali, Chandigarh, India

***ABSTRACT— The proposed model is based upon the WSN routing to resolve the routing related issues in the traditional WSN networks. This model is designed with dynamic network routing to predict the trust value of the sensor node. This trust values helps the routing algorithm to take decision on involvement of the node in the appropriate path. The idea behind the trust value is to eliminate the attack nodes from the routing paths in the network cluster, which is supposed to improve the network performance. In most of cases, the major reason behind data drop in sensor networks lies in the network attacks, connectivity holes and non-target nodes influenced by the network attacks. The proposed dynamic network routing is designed on the basis of three performance parameters, which includes the transmission delay, throughput and distance. These parameters are classified in the terms of low, medium or high, and the different combinations of these parameters returns the different trust values of network nodes. A sensor node is typically classified in five categories, which involves very high, high, medium, low and very low options. The dynamic network routing based routing model is combined with Dijikstra'a shortest path algorithm to discover the shortest and smartest paths among the given network segment. The proposed model is designed with aim to improve the overall performance of the sensor networks by eliminating the attack nodes. This model verifies the trust value of each next-hop node, when choosing the path between sources and destinations.***

***KEYWORDS—Smart City routing, Optimized routing, Shortest path first, smart path.***

## 1. INTRODUCTION

It is hard to establish a common ground for IOT standards for the evolution of the IOT reference architecture. As proposed by[2] a Reference Architecture Model for IOT provides a model for the transmission between many heterogeneous IOT devices and the Internet as a whole.

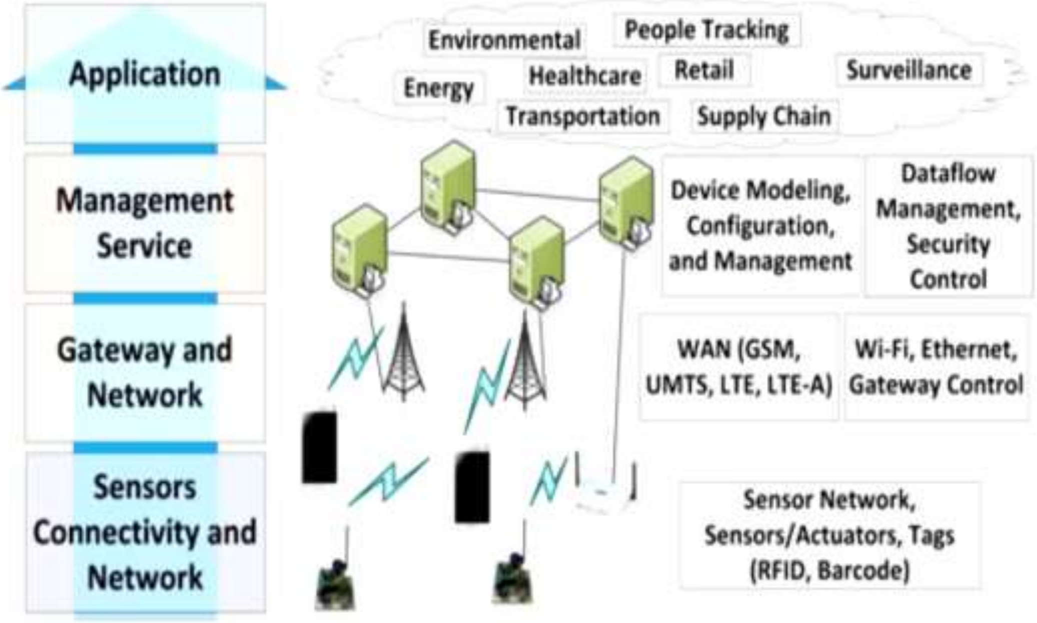
Application
Management Service
Gateway and Network
Sensors Connectivity and Network
Environmental
People Tracking
Energy
Healthcare
Retail
Surveillance
Transportation
Supply Chain
Device Modeling, Configuration, and Management
Dataflow Management, Security Control
WAN (GSM, UMTS, LTE, LTE-A)
Wi-Fi, Ethernet, Gateway Control
Sensor Network, Sensors/Actuators, Tags (RFID, Barcode)

Figure 1: IOT Architectural Layers [30]

Each device in the network contains IP address which unambiguously identifies it on the internet. The physical layer contains sensor devices ex RFID, barcode, Actuators, which are used to collect real time information and make use of low power and low data rate. It requires strong and authentic performance for the private, public or hybrid network model. Thus network models are designed to communicate QoS requirements for latency error, probability, scalability and bandwidth, security while achieving high level of energy efficiency. Information analysis, security control, process modelling and device management are contained in Management service layer .

In application layer various small and industry sector use IoT for service enhancement. This can be classified by courage, size, availability, heterogeneity and business model. Areas like personal and homes, utility, enterprise, mobile etc are included.

Human services applications introduce a few difficulties: low power, restricted calculation, material limitations, persistent operation, heartiness and adaptation to internal failure, versatility, security and obstruction, and administrative prerequisites. The power challenge is available in practically every territory of utilization of remote sensor systems, yet restriction of a keen sensor embedded on a man still stances significantly additionally challenge, albeit progressing research tries to give control remotely. Another test as far as power originates from the operational warmth. For example, at times it is impractical to chill off the sensor by permitting contact with the earth. A commonplace soluble battery, for instance, gives around 50 watt-hours of vitality. This may mean not as much as a time of ceaseless operation for every hub in full dynamic mode. By and by, for some applications, it will be important to guarantee that a system can stay operational with no substitutions. Calculation is specifically restricted because of the constrained measure of energy. Ordinarily, bio-sensors are not anticipated that would have an indistinguishable computational power from traditional Internet of Things hubs. Since correspondence is indispensable and impression is little, little power stays for calculation. An answer can be information combination, which involves a few hubs pooling their data together for expanded computational power handling and precision. Additionally, it might be normal that for a few applications, for example, blood glucose checking, the capacity to transmit information to an outer gadget will be required for encourage information handling. A few sensors may have differing capacities that speak with each other and convey one community information message. Material requirements is another issue for remote sensor systems application to medicinal services. A biosensor must be in contact with human body, or even on it. In the event that the biosensor is inside a pill, the decision of development materials must be cautious, particularly on batteries. Likewise compound responses with body tissue and the transfer of the sensor is of most extreme significance. In numerous applications, it is conceivable to dispose of at least one brilliant sensors without the requirement for any administrator intercession. Ceaseless operation must be guaranteed along the life cycle of and openings. The regularly inspiration for aggressor is advantage from information. Aggressor openings extend from physical get to, remote correspondence, assaults on coordination and self-design, up to organize perceivability. Administrative necessities should dependably be met, significantly more with medicinal applications. There must be some confirmation that these gadgets won't hurt; even model gadgets should meet the strict guidelines of patient security before any human testing should be possible. The remote information transmission must not hurt human body and the incessant working and power usage of these gadgets should likewise be kind. Plan for security must be a key component of biomedical sensor advancement, even at the soonest arranges. Sensible confirmation of plan viability will be required notwithstanding for model gadgets.

## 2. LITERATURE REVIEW

Renita Machado [13] IOT networks (IOT) including tiny knots, limited powers are gained the higher popularity in the data collection applications. The potential of IOT models is quite higher, which is characterized by its flexibility, scalability and high adaptability to the versatile environments. Although these environments detection targets are unique and depends on the application, the criteria of common performance for IOT networks extends the service life while satisfying the network coverage and connectivity in the deployment area. Pau Closas [8] in this paper, the issue of control of the network topology using a totally distributed algorithm is considered in wireless networks. While the proposed distributed algorithm is designed applying the concepts of game theory to implement a non-cooperative game, network connectivity is possible on the basis of asymptotic results of network connectivity. Yenumula B [18] the problem of sensing malicious nodes in IOT networks is considered in this paper. So current safety mechanisms are inadequate for IOT networks, in this article the author should develop a new environment to sense malicious nodes using Zero-Sum game technique and selective acknowledgments node in the path data forward. Harilton da S. Araújo et al. [6] proposed a protocol to reduce energy consumption in the network by changing the protocol called Directed Diffusion routing protocol. The proposal uses a Geocast approach in which all the broken roads are repaired by rebuilding new route computation tree so that the energy cost can be reduced. Abdellah et.al [1] propose a hierarchical protocol called Adaptive of effective and balanced energy Routing Protocol (from HABRP) to decrease the probability of failure of nodes and prolong the time interval before the death of the first node (stable period) and the increase in lifespan heterogeneous IOTs, which is crucial for many applications. Bomgni Alain Bertrand et al. [3] propose an algorithm which is based clique. This algorithm guarantees the delivery of packets sent by the receiving node to all nodes that are deployed in various Geocast regions. In this proposal, the proposed algorithm is a hybrid classification system.

## 3. EXPERIMENTAL DESIGN

The IoT network is the next generation network of things and is gaining popularity day by day because of its multiple and wide usage. The issue of IoT network route handling is being addressed in the proposed project work. The proposed work in based on the unique combination of mathematical random function to generate the key table. The smart routing table generation and management mechanism used in the proposed work in based on the unpredictable key relationship theory, where the stronghold formula based route relationships will be incorporated to manage the data routing. The proposed work is based on the adaptive smart routing mechanism, which means that every node will be able to handle its key exchange policy with the receiver node during every call setup. In this way, every sender node will be made capable of insuring the integrity of the data propagation in the given IoT network.

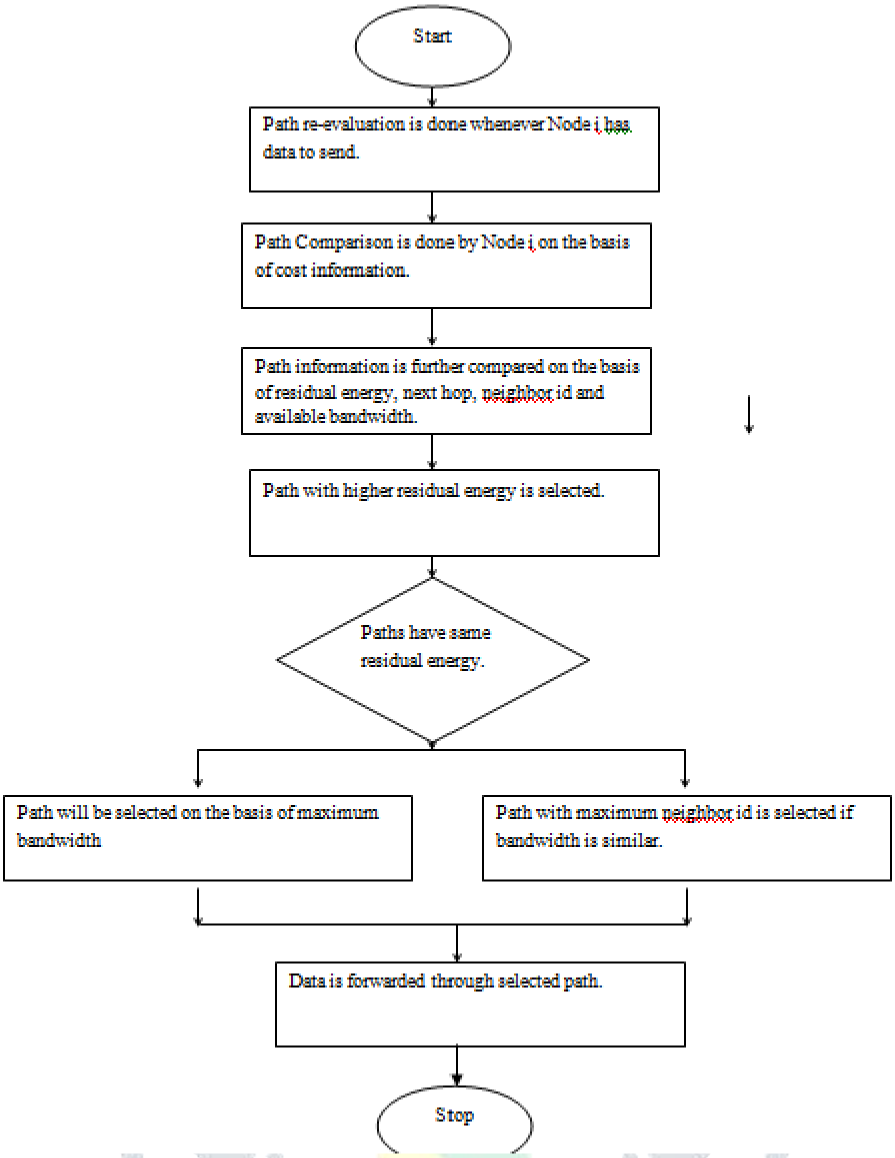
Start
Path re-evaluation is done whenever Node i has data to send.
Path Comparison is done by Node i on the basis of cost information.
Path information is further compared on the basis of residual energy, next hop, neighbor id and available bandwidth.
Path with higher residual energy is selected.
Paths have same residual energy.
Path will be selected on the basis of maximum bandwidth
Path with maximum neighbor id is selected if bandwidth is similar.
Data is forwarded through selected path.
Stop

Figure 2: Smart Node Evaluation and Path Discovery Algorithm

The proposed model has been embedded with multiple node discovery option altogether in order to find the stable and best performing path between the source and destination nodes. The performance of the network segment is evaluated using the variety of performance parameters, which includes the data volume and network packet delivery models (throughput and packet delivery ratio), network efficiency (in the terms of network load, packet efficiency), time based assessment in the form of transmission delay. The proposed model is employed using the MATLAB framework, where the graphical representation has been demonstrated in the multiple formations. This model relies upon the node availability assessment through ping/pong method, where ping is used to query the node, and pong is received back from the nodes in response to each ping received in the wireless sensor networks.

## 4. RESULT ANALYSIS

The comparative analysis of the proposed and existing models has been performed on the basis of latency and throughput based parameters. The latency is known to describe the time taken for the travel of data over the given path, whereas the throughput depicts the capacity of the network to process certain amount of data in given time. The tables and figures to represent the comparative results are described in the following section.

The values of latency are observed for both existing and proposed models, as its shown in figure 1. The significant difference has been observed between the existing and proposed models at all of the events. The maximum value of latency for the existing model is observed at 0.019 seconds in comparison with proposed model (0.0023 seconds). The existing model is observed with 0.000182 seconds of latency against the 0.00012 seconds of the proposed model. This shows the certain improvements in the proposed model on the basis of the latency.

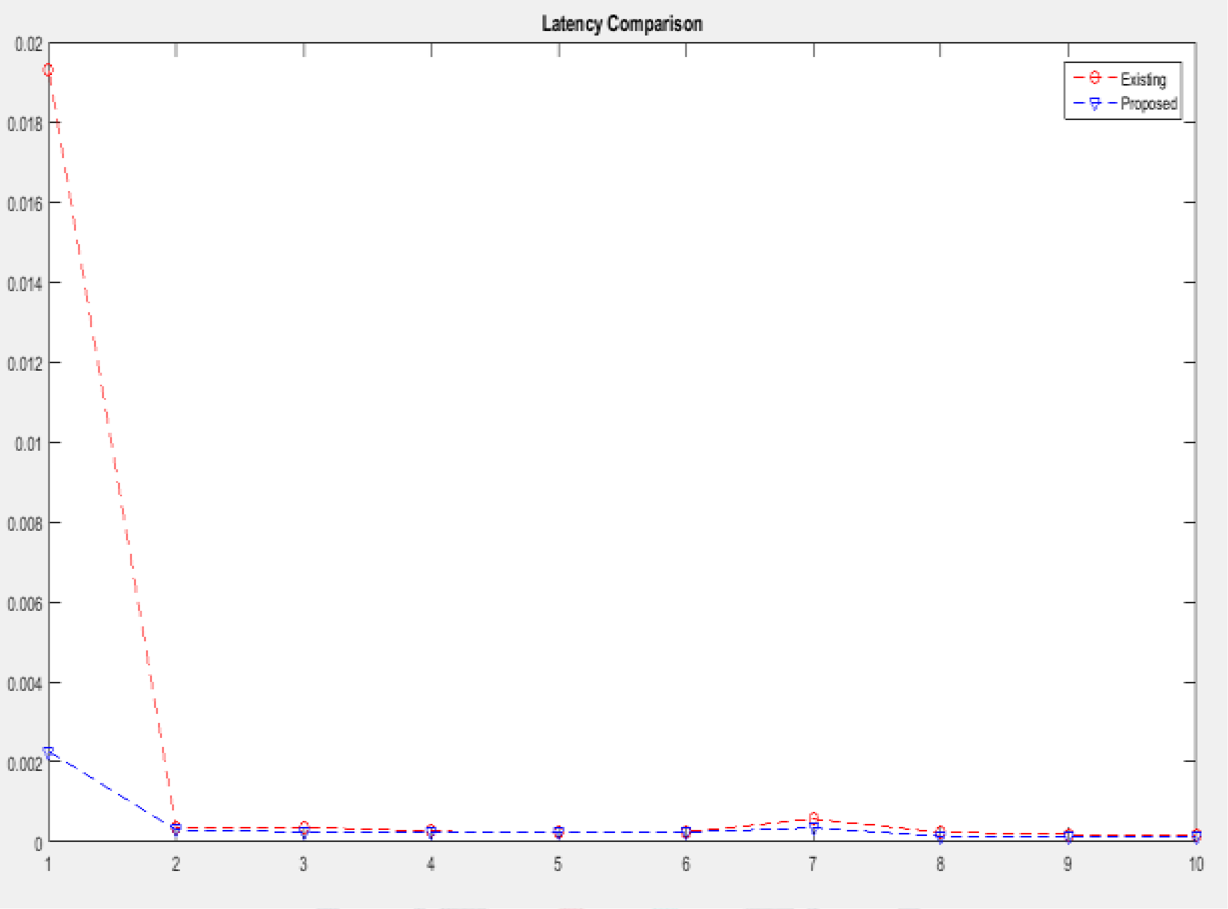

Figure 3: The comparative analysis based upon latency is shown in this figure

The above figure describes the clear comparison between the existing and proposed models. The proposed and existing models are significantly identical after the first event. However, the proposed model is consistently observed significantly lower than (or almost equal to) the existing model. This shows the significant performance of the proposed model in comparison with the existing model.

The figure 2 considers the comparison of existing and proposed model on the basis of the throughput parameter. The improvement of the proposed model is considerably higher than the existing model on all of the events, except the first event. The first event for the existing model is described with value 0, which is due to the non-existent traffic at given event. However, in the random explanation, the proposed model is observed with 90 Kbps against the 80 Kbps in the existing model on the 5th event. On 10th event, the proposed model's observation of 95 Kbps against 90 Kbps of existing models. The proposed model is observed with average value of nearly 85 Kbps against the existing model (80 Kbps), which shows the high efficiency of the proposed model in transmitting the data between the wireless nodes.

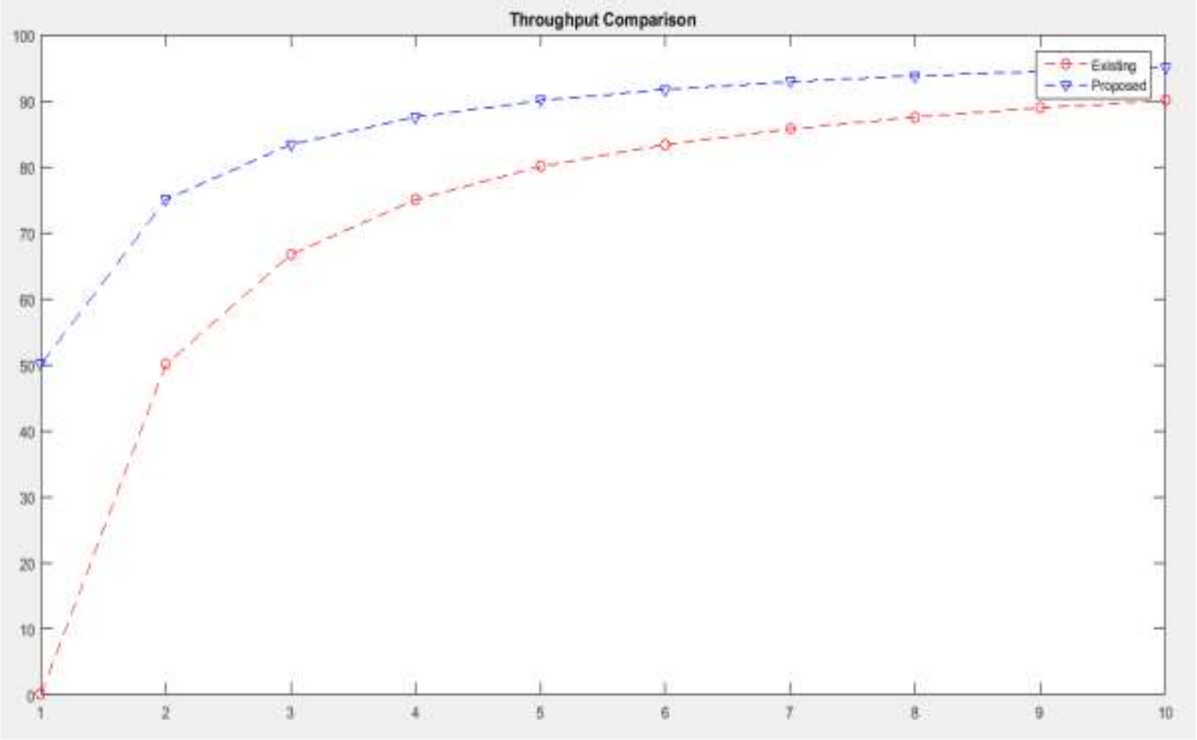

Figure 4: The comparative analysis based upon throughput is shown in this figure

The above figure shows the existing and proposed model performance based upon the throughput parameter. The proposed model is consistently observed higher than the existing model on the basis of figure 1 however the difference is narrowed down with each network event.

## 5. CONCLUSION

The performance of the proposed model is analyzed and compared on the basis of PDR and end-to-end delay parameters. The proposed model is found better nearly on all simulation events in the terms of PDR. The PDR in this simulation is recorded between 99 and 99.99 percent. The average value of PDR is recorded at 99.19%, which is improved than existing model (98.93%). The minimum PDR based comparison proves the efficiency of proposed model (99%) against the existing (98%) on the standard WSN simulation. The performance on the basis of end-to-end delay is recorded below 0.01 seconds on all of the simulation events for proposed model, which is significantly proved by end-to-end delay of existing model with greater value than 0.01 seconds on all simulation events. The average transmission delay is recorded significantly lower in proposed model (0.0004 seconds) in comparison with existing model (0.04 seconds). In the future, this model can be further improved with complex Dynamic network routing with more rules for trust calculation among the network nodes. The ontology described over node information, network performance, type of service and other parameters can be used with machine learning for classification of sensor nodes.

## REFERENCES

[1] Agah, A., Asadi, M., & Das, S. K. (2006). Prevention of DoS Attack in Mesh networks using Repeated Game Theory. In *ICWN* (pp. 29-36).

[2] Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless mesh networks. *Ad hoc networks*, *3*(3), 325-349.

[3] Alain Bertrand, B., & Jean Frédéric, M. (2010). An energy-efficient clique-based geocast algorithm for dense mesh networks. *Communications and Network*, *2010*.

[4] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless mesh networks: a survey. *Wireless communications, IEEE*, *11*(6), 6-28.

[5] Ben Alla, S., Ezzati, A., Beni Hssane, A., & Hasnaoui, M. L. (2011, April). Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless mesh networks. In *Multimedia Computing and Systems (ICMCS), 2011 International Conference on* (pp. 1-6). IEEE.

[6] Briles, S., Arrowood, J., Turcotte, D., & Fiset, E. (2005, May). Hardware-In-The-Loop Demonstration of a Radio Frequency Geolocation Algorithm. In *Proceedings of the Mathworks International Aerospace and Defense Conference*.

[7] Byers, J., & Nasser, G. (2000). Utility-based decision-making in wireless mesh networks. In *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on* (pp. 143-144). IEEE.

[8] Closas, P., Zamora, A. P., & Rubio, J. A. F. (2009, April). A game theoretical algorithm for joint power and topology control in distributed WMN. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* (pp. 2765-2768). IEEE.

[9] Dai, H., & Han, R. (2003, December). A node-centric load balancing algorithm for wireless mesh networks. In *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE* (Vol. 1, pp. 548-552). IEEE.

[10] Dufwenberg, M., & Kirchsteiger, G. (2004). A theory of sequential reciprocity. *Games and economic behavior*, *47*(2), 268-298.

[11] Han, Z. (2012). *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press.

[12] Ishmanov, F., Malik, A. S., & Kim, S. W. (2011). Energy consumption balancing (ECB) issues and mechanisms in wireless mesh networks (WMNs): a comprehensive overview. *European Transactions on Telecommunications*, *22*(4), 151-167.

[13] Machado, R., & Tekinay, S. (2008). A survey of game-theoretic approaches in wireless mesh networks. *Computer Networks*, *52*(16), 3047-3061.

[14] MacKenzie, A. B., & DaSilva, L. A. (2006). Game theory for wireless engineers. *Synthesis Lectures on Communications*, *1*(1), 1-86.

[15] Meshkati, F., Poor, H. V., & Schwartz, S. C. (2007). Energy-efficient resource allocation in wireless networks. *Signal Processing Magazine, IEEE*, *24*(3), 58-68.

[16] Park, G. Y., Kim, H., Jeong, H. W., & Youn, H. Y. (2013, March). A novel cluster head selection method based on K-means algorithm for energy efficient wireless mesh network. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 910-915). IEEE.

[17] Petrovic, D., Shah, R. C., Ramchandran, K., & Rabaey, J. (2003, May). Data funneling: Routing with aggregation and compression for wireless mesh networks. In *Mesh network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on* (pp. 156-162). IEEE.

[18] Reddy, Y. B., & Srivathsan, S. (2009, June). Game theory model for selective forward attacks in wireless mesh networks. In *Control and Automation, 2009. MED'09. 17th Mediterranean Conference on* (pp. 458-463). IEEE.

[19] Sakarindr, P., & Ansari, N. (2007). Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless mesh networks. *Wireless Communications, IEEE*, *14*(5), 8-20.

[20] Sarkar, S., & Datta, R. (2014, February). A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks. In *Communications (NCC), 2014 Twentieth National Conference on* (pp. 1-6). IEEE.

[21] Seada, K., Helmy, A., & Govindan, R. (2004, April). On the effect of localization errors on geographic face routing in mesh networks. In *Proceedings of the 3rd international symposium on Information processing in mesh networks* (pp. 71-80). ACM.

[22] Seada, K., Zuniga, M., Helmy, A., & Krishnamachari, B. (2004, November). Energy-efficient forwarding strategies for geographic routing in lossy wireless mesh networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 108-121). ACM.

[23] Shi, H. Y., Wang, W. L., Kwok, N. M., & Chen, S. Y. (2012). Game theory for wireless mesh networks: a survey. *Sensors*, *12*(7), 9055-9097.

**[24]** Stojmenovic, I., & Lin, X. (2001). Power-aware localized routing in wireless networks. *Parallel and Distributed Systems, IEEE Transactions on*, *12*(11), 1122-1133.

**[25]** Upadhyayula, S., & Gupta, S. K. (2007). Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced convergecast (dac) in wireless mesh networks. *Ad Hoc Networks*, *5*(5), 626-648.

**[26]** Wagner, R., Sarvotham, S., Choi, H., & Baraniuk, R. (2005). *Distributed multiscale data analysis and processing for mesh networks*. RICE UNIV HOUSTON TX DEPT OF ELECTRICAL AND COMPUTER ENGINEERING.

**[27]** Xu, J. Q., Wang, H. C., Lang, F. G., Wang, P., & Hou, Z. P. (2011, June). Study on WMN topology division and lifetime. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on* (Vol. 1, pp. 380-384). IEEE.

**[28]** Yadav, S., & Lakhani, K. (2013). A Cluster based Technique for Securing Routing Protocol AODV against Black-hole Attack in MANET. *International Journal of Distributed and Parallel Systems*, *4*(2), 17.

**[29]** Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless mesh networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, *35*(3), 867-880.

**[30]** Zhao, L., Zhang, H., & Zhang, J. (2008, March). Using incompletely cooperative game theory in wireless mesh networks. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE* (pp. 1483-1488). IEEE.

**[31]** Agah, A., Asadi, M., & Das, S. K. (2006). Prevention of DoS Attack in Mesh networks using Repeated Game Theory. In *ICWN* (pp. 29-36).

**[32]** Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless mesh networks. *Ad hoc networks*, *3*(3), 325-349

**[33]** Al-Saadi, Ahmed, Rossitza Setchi, Yulia Hicks, and Stuart M. Allen. "Routing Protocol for Heterogeneous Wireless Mesh Networks." *IEEE Transactions on Vehicular Technology* 65, no. 12 (2016): 9773-9786.

**[34]** Murugeswari, R., S. Radhakrishnan, and D. Devaraj. "A multi-objective evolutionary algorithm based QoS routing in wireless mesh networks." *Applied Soft Computing* 40 (2016): 517-525.

**[35]** De Domenico, Manlio, Antonio Lima, Marta C. González, and Alex Arenas. "Personalized routing for multitudes in smart cities." *EPJ Data Science* 4, no. 1 (2015): 1.

**[36]** Zhou, Anfu, Min Liu, Zhongcheng Li, and Eryk Dutkiewicz. "Cross-layer design with optimal dynamic gateway selection for wireless mesh networks." *Computer Communications* 55 (2015): 69-79.

**[37]** Ganichev, Igor, Bin Dai, P. Godfrey, and Scott Shenker. "YAMR: Yet another multipath routing protocol." *ACM SIGCOMM Computer Communication Review* 40, no. 5 (2010): 13-19.

**[38]** Xu, Wen, and Jennifer Rexford. *MIRO: multi-path interdomain routing*. Vol. 36, no. 4. ACM, 2006.