International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I1P205
Volume 69 Issue 1, 29-34, January 2021
© 2021 Seventh Sense Research Group®

An Improved Zone Routing Protocol For Secure And Efficient Energy Management

[#1]Kollu Spurthi, [#2]T.N.Shankar
Research Scholar[#1], Professor[#2]

Dept of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, AP, India.

kolluspoorthy03@gmail.com, tnshankar2004@rediffmail.com

Abstract *— Many researchers, despite their contribution towards technology reflecting ad hoc networks like MANETS, left a few stones unturned, thereby giving scope for enhancement and research in this area. MANET is dynamic without the aid of wired infrastructure, ought to rely on its core operation Routing. Routing protocols are inevitable for the transmission of data between nodes. The characteristics of MANET's fabricate their design as a challenge. The Legacy studies on Literature resulted in innumerable protocols categorized as Proactive, Reactive, and Hybrid. This paper put forth's an enhanced Zone Routing Protocol that hinges on security, clustering, and Energy efficiency that is more stable and shows effective performance than traditional ZRP. Our proposed model depends on the clustering algorithm, attribute-based encryption, and fuzzy classification to reduce energy consumption, routing overhead, and increase security. Results of NS3.2 simulation illustrates that enhanced ZRP shows high-performance indexes in various QoS parameters like throughput, End to end delay, Load balancing, Energy consumption, and Delivery ratio concerning existing ZRP.*

Keywords — *MANET; Network security, ZRP, ABE, QoS Parameters.*

I. INTRODUCTION

Manet, otherwise known as a Mobile ad hoc network by its nature, does not have a fixed infrastructure. Manets occupied their research place since the mid-1990s and still evolving, encroaching on various aspects of concern like routing security, transmission medium, and many more. The free-moving nature of nodes in a network resulting in topology change makes it a preferred and adaptable network in various wireless areas. Devices in this type of network are free to join and leave the network on the fly[20].

This network, which reacts spontaneously to changing environments, has its mark in army tactical networks. Other applications include Air force, Disaster Management, Data Mining and spying hospital administration, spying IoT-based smart homes, etc. All the fore mentioned applications turn around the key for transferring data between nodes[19]. Routing, a vital label for communication, has put its mark in research. Routing, a centric parameter for any network irrespective of wired or wireless, shows different features based on the network environment. Wireless networks employ pressure on researchers for designing protocols in environments of node movement and topology transformations. Routing, a standstill challenge in the survey for the past few years, has been under rigorous study and resulted in numerous mature protocols categorically termed as proactive, reactive, and hybrid protocols [15]. The aliasing names for proactive and reactive are table-driven and on-demand protocols, respectively. This category of table-driven protocol maintains an updated list of targeted nodes and their respective routes by exchanging and distributing routing tables at intervals. These proactive protocols offer quick discovery of routes with reliability at high data maintenance costs and delayed response on reconstruction and failures. Routing algorithms like DSDV, OLSR, and WRP fall into this category. The basic principle of Reactive protocols like AODV, AOMDV, DSR, TORA, etc., is timely notifying routing information based on the requirement [13,1]. One more category reflecting a combinational behavior is hybrid, including ZRP, CEDAR, and FSR, out of which ZRP is considered for our work [3]. MANET's are gaining attention as their real-time application is worth pouring advantages and ease of use of technology. But a challenge shadowing MANET's performance is its Qos parameters like bandwidth, lowering packet loss, delay in transmission, security thumbnails, etc. Implementing QoS in MANET's is constrained by its characteristic features of decentralized infrastructure, limited availability of resources, unstable modes in terms of physical placement, higher energy requirements pave scope for development and evolution of improved technology.

Our objective is to put a limelight on ZRP, the preferred hybrid routing protocol with regulating QoS factors, namely energy efficiency, throughput, Latency, Packet drop, and security aspects. The Proposed framework supports Authentication service over a secured transmission network with a reduction in energy consumption. We validate our analytical results with simulations.

II. RELATED WORK

Many authors shared their inventions in various publications that are surveyed as base preliminaries of related work. The contributions are review in the following section. In 2016, Mr. Honda Moudni and Mohomed Er-Rouidi [1] came up with issues related to the security of routing protocols in MANET's being classified as

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

cryptography-based, one-way hash chain based and hybrid methods and their implementation. According to A. Subramaniam [2] in 2003 presented a technique for lowering power consumption in ZRP by splitting the zone with two power levels. Ms. Swati Sharma et al. in 2016 proposed a modified ZRP, which included additional variables to deal with the reduction of co-operative attacks. Her proposed model was based on the fuzzy approach [3]. Ms. Deepa Mehta addressed route aggregation problems by improving its QoS parameters leading to [4] Energy Enrichment in MANETs in 2017. Mr. Leonard Barolli, Mr. Yosshitaka Honma et al. in 2017 proposed a Border-Casting zone routing protocol [5], which reduces the load at networks. Mr. Phamthi Minh Thui et al. have advocated a new approach named LAZRP to reduce routing overhead and end delay in 2015 [6]. Mr. Samuel Chrllathirrai has [7] propounded evolutionary zone routing protocol in 2013 that is an extension to ZRP, which improves a network's performance. This approach applies to outer zones. Ms. Shwetha R. Malwe, the IEEE member, proposed selective broadcast to reduce storage complexity of routing table and control [8] overhead in 2016. In the same year [9], Osama A. Awad, Marim Rushdi directed a fuzzy logic implementation on ZRP, resulting in the network's extended lifetime. [10] Varun Kumar Sharma et al. proposed an ejective fuzzy-based energy efficient load distribution scheme that considers congestion as a vital parameter, with increasing network lifetime, throughput energy of nodes. [11] Sazzat Hossain in 2019 proposed a merging technique to avoid a Blackhole attack in MANET's. Merge technique included both SHA3 and Diffie-Hellman algorithm[13]. TN Shankar in 2016 proposed IDS in Manets using ElGamal digital signature in AODV[13], and 2019 came up with research work on wormhole attack[14]. Rajinder Singh et al. [15] in the year 2014 proposed a technique to implement a security-enhancing algorithm for Mobile Adhoc Networks. Shivendra Prakash, in his paper, talked about ZRP's several techniques to overcome the black hole attack in ZRP in the year 2016 [16]. Kamalakanta Sethi in 2019 contributed to a hierarchal approach based on attribute cryptosystem to compensate for adverse effects of overhead[17]. Nanli in 2010 gave a comparative study o efficiency of various authentication methods and proposed an improved key exchange method for deficiency Helman protocol[18]. Mr. Mirjeta Alinci et al. in the year 2015 contributed an informative survey on clustering schemes that can be applied on manets[19]. In 2011, Sheetal Mehta talked about various clustering schemes with their performance metrics[20]. Xueqin Yang et al. in the year 2018 proposed a protocol based on clustering combined with ZRP to enhance ZRP performance.[21]. Shyam Singh Rajput et al. in the year 2014, proposed SEZRP with more mal for the confidentiality of messages, arising at minimizing key sharing overhead[22].

III. BASIC IDEA OF ZRP

The Zone Routing Protocol (ZRP) [7], a hybrid framework, characterizes Intra, and inter-zone communication paths. If the packet is to be transferred within a zone, the proactive approach has opted. When the packet is destined to other zones, the reactive protocol comes into operation, thereby routing the packet to its intended destination [5]. ZRP works using three protocols IARP, BRP, and IERP [6].

IARP [4] uses a proactive approach to identify the neighbor within the zone by sharing a copy of the updated routing table with nodes in the zone periodically [8]. The path established between the nodes is accessible immediately, which reduces the overhead and latency of the network

IERP protocol uses a reactive approach for the transmission of data in inters zones [4]. Peripheral nodes are regular nodes with the added responsibility of transferring data to different zones [21, 16] using Border Resolution protocol [9]. Query packet from the source node is transmitted to the entire mobile network zones using a broadcast tree. IERP is responsible for route establishment from the source to the intended destination node.

Energy efficiency, attacks, and misbehavior of nodes affect the growth and execution of ZRP. Despite the strong framework on which ZRP is built, the factors above directly or indirectly deteriorate the network performance to fall below a minimum threshold. To implement the intended functionality and uphold the breakeven point, there is a need to design a realistic framework where effecting parameters are nullified for leveraged results.

IV. EFFECTING PARAMETERS

The influencing factors of energy efficiency[2,10] that may be optimized for energy consumption are factors like improving node count, speed, changing data rates of traffic, increasing node lifetime, and further. Security factors entailing attacks decline the network's performance and reliability by dropping packets, creating the illusion of the shortest path [12], and blocking communication between nodes. Few such attacks to be considered are the Sinkhole attack, the Wormhole attack[14], the Blackhole attack, the Grey hole attack, the Jellyfish attack, the Packet dropping attack, the Stealthier attack, etc.

The above-mentioned attacks ping on to MANET routing's causing several degradation and failures within the network [15]. To handle subsequent attacks, energy parameters, and optimization in routing enhanced ZRP is proposed for our research work. ABE, in combination with Diffie-Hellman, is picked as an add-on for security enhancement.

Paragraphs must be indented. All paragraphs must be justified, i.e., both left-justified and right-justified.

A. ABE [Attribute Based Encryption]:

ABE, asymmetric encryption uses a pair of public and private keys [17]. Here the secret key of the sender and receiver is used to transform plan text to the ciphertext and vice versa, depending on attributes related to a node. This encryption property enables security features, namely authentication, access control, integrity, and confidentially

[22]. The vital security-based feature of ABE is resistance to collisions with 2 types of ABE Schemes. In our system, we considered key policy-based ABE, hands-on with Deffie Hellmen key exchange [11].

The attributes of nodes used for computation with the ABE algorithm are pipelined to the Diffie- Hellman key exchange algorithm to retrieve the respective Public and Private Key pairs used to secure the data during transmission. Diffie- Hellman algorithm [18] allows both the communicating parties to agree upon terms supporting private communication over a public network with an independent encryption method of their wish.

Diffie-Hellman Key Exchange:

1. Prime number 'p', primitive root 'm' (1<=m<=p)
2. Node A : choose prime(A) i public (A) = m ^ i mod p
3. Node B: choose prime(B) j Public (B) = m ^ j mod p
4. Public keys are communicated between both parties A and B.
5. Node A: exchanged private key, K1= public (B) ^ prime (A) = m^ j i mod q
6. Node B: exchanged private key, K1= public (A) ^ prime (B) = mi ^ j mod q.

V. PROPOSED FRAMEWORK:

Enhanced ZRP relies on increasing node lifetime using fuzzy classification, clustering for reducing overhead, and encryption algorithm to face various attacks that degrade the network's performance and reliability.

ZRP, our focussed and opted hybrid routing protocol, has high potential in grabbing the researcher's attention. This protocol, despite its efficiency in shifting among the two IARP and IERP, thereby improving latency and ease of control, suffers from the black mark of high power consumption, which is addressed in our proposed work. Our paper serves as a mechanism to retain the well-expected performance of ZRP, still proposing an admitted lowering in energy consumption. These two factors define and leverage the network's lifetime. The proposed work initiates with networks divided into clusters using some opted function and selecting a cluster head. This selection is made relying on factors like distance between nodes and their energy levels, .i.e. the node that is closer in the distance to all the nodes and holding higher energy levels will become the cluster head.

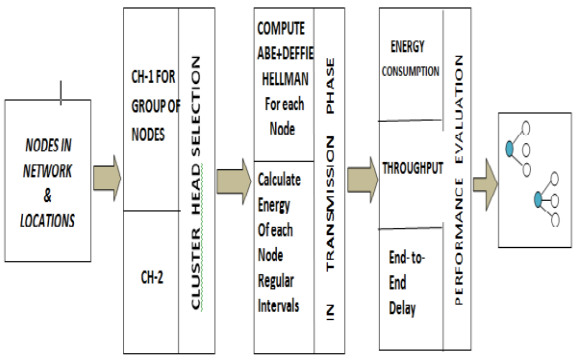

Fig 1. A sequence of the Proposed framework

Fig 1 consists of 3 crucial steps: Cluster Head Selection, Security Phase, and Performance evaluation. Arrow depicts the flow of data between these phases

The algorithm converges as below in several steps:

1. The network is divided into clusters based on the Euclidean distance between nodes.
   $ED = \text{sqrt } (x2-x1)^2 + (y2-y1)^2$
2. Each cluster elects a cluster head considering two parameters, distance, and Energy.
3. The Energy of each node is calculated for the predefined interval.

$$\text{Energy} = P_N \quad X \quad t$$

Where P_N is transmitting and Receiving Power and t is time.

$t = 8$ X Packet length/B_w, B_w is Bandwidth.

As a node transmits a packet, energy consumption is computed as the sum of the receiving and transmitting packet.

$$E_t = E_{tr} + E_{RC}$$

E_{tr} is the Energy of transmission and E_{RC} Energy of receiving.

$$E_{tr} = E_{con} * M + E_R * M * d^2$$

E_{con} Energy consumed, M is a number of bits, d is the distance, E_R is Energy for routing.

$$E_{RC} = E_{tr} = E_{con} * M$$

4. Routing between clusters is done with peripheral nodes' help by targeting RREQ packets to these nodes to transmit data outside clusters.
5. During information sharing, each node computes a secure secret key using ABE considering node attributes like location, bit rate, and packet length. key generated as

$f(x,y) = \text{Sum } (x^i y^j)$, where $(q_{ij}=q_{ji})$ and i,j between 0 and N

Q is a large prime number, i cryptographic key, j common key generated.

6. The Computed secret key is shared with the Diffie - Hellman key exchange to ensure the integrity and the authentication key are computed regularly.
7. To increase node lifetime, owing to energy optimization, energy is calculated for every node with predefined threshold time, which is classified into α,β,γ phases using fuzzy classification. If a node receives an RREQ packet, it computes its energy level. It holds the packet for the particular period inversely proportional to the energy level employing a concave delay mechanism.

$$\text{Delay}=(e^2+d^2)/2+d-\text{sqrt}((d^2+e^2)/2 \text{ X } d - (Mc-e^2))$$

Where e= maximum Energy, d =Minimum delay, and Mc is current Energy.

From the literature, the Delay mentioned above function reflects optimal performance. In our simulation, we use the following delay function.

$$\text{Delay} = d+(5/(e+5))$$

Where e is Energy and d is a delay, i.e., the Concave delay function is considered for our simulation.

A. Performance evaluation and analysis:`

To Implement the Proposed hybrid approach using NS2, the Simulation parameters are initialized as shown in table1. The performance of ABE-ZRP is analyzed with ZRP by considering the parameters throughput, Load Balancing, Energy consumption, End to End Delay, and Delivery ratio.

Throughput indices the delivery rate of transmitted packets within the stipulated time. More the throughput betters the performance.

End to end delay services the average time-lapsed which includes delay during transmission from source and destination.

Packet Delivery Ratio is considered the ratio measured between packets transmitted and packets received at the destination, resulting in high performance.

Table 1: Simulation Parameters

PARAMETERS	VALUES
Simulator	NS3.2
Simulator Time	100s
Simulation Area	1000*1000 m
Proposed Protocol	hybrid approach
Initial Energy of nodes	1J
Number of Nodes	33
Bit Rate	1Mb/sec
Packet Length	500 byte

B. OBSERVATIONS

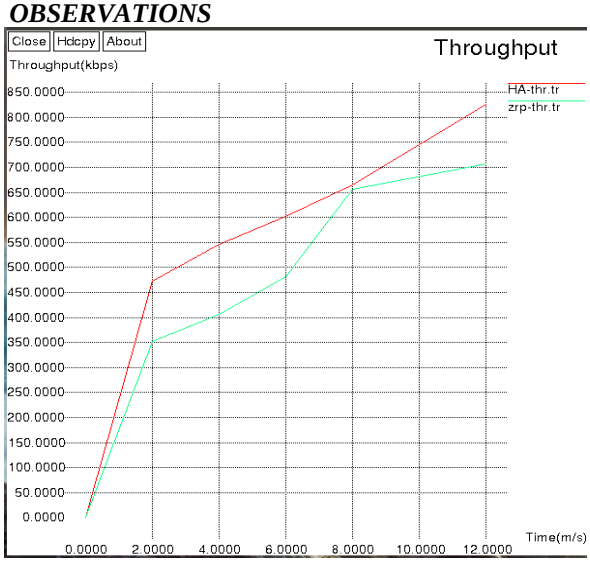

Fig 2.Throughput of ZRP Vs. ABEZRP

we compared the proposed schema with ZRP as shown in fig 2, and underlying results showed improved throughput on the scale of X graph with a red spike for HA and green spike for ZRP

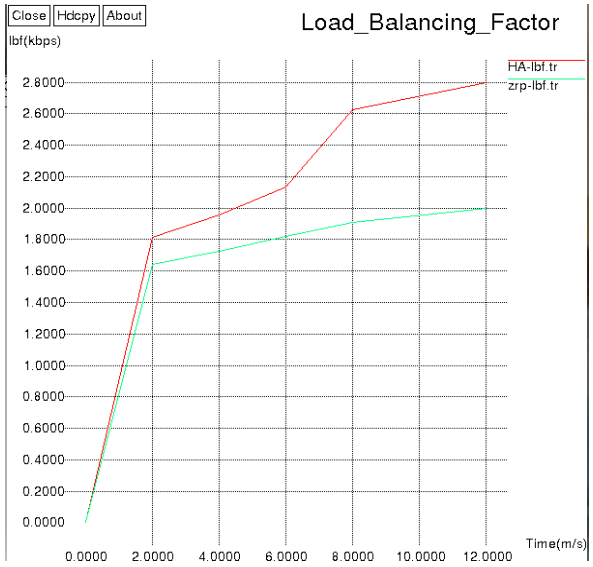

Fig 3. Load Balancing of ZRP Vs. ABEZRP

The above fig 3 reflects load balancing calculated for both ZRP and ABE –ZRP with red and green spikes, respectively. Improved Load balancing is obtained for the later one.

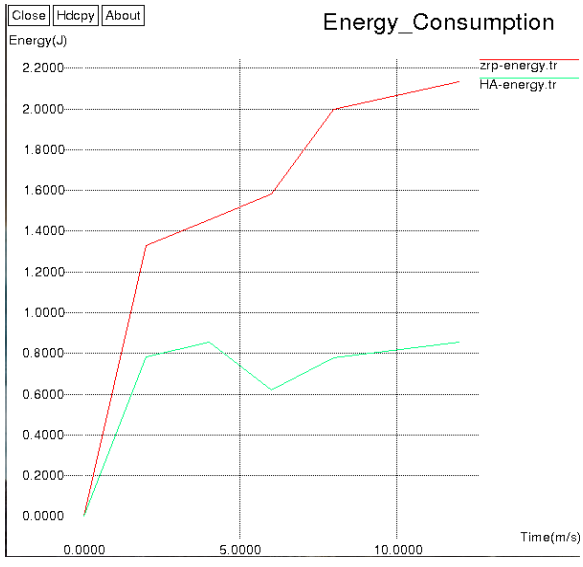

Fig 4.Energy Consumption of ZRP Vs. ABEZRP

The above Fig 4 depicts a lowered Energy consumption by our proposed model indicated with a red spike over green spike for ZRP, an important design criterion in Manets.

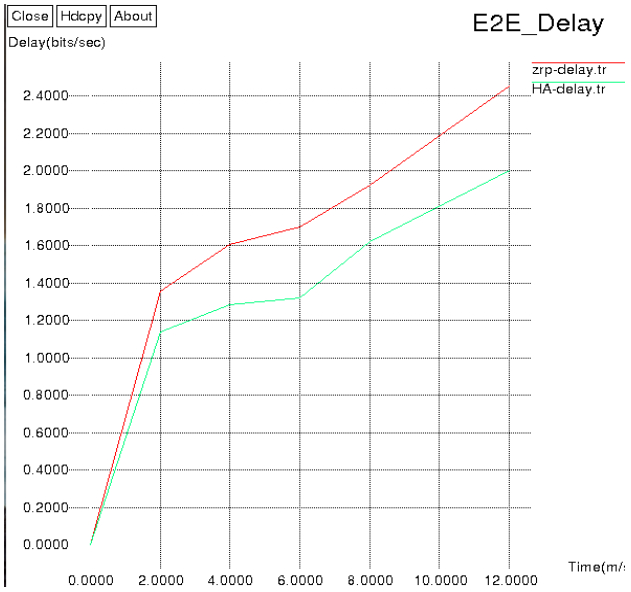

Fig 5. E2E Delay of ZRP Vs. ABEZRP

In Fig 5, our proposed system reveals reduced End to End delay with a green spike for HA compared with a red spike representing ZRP, exhibiting a longer delay during transmission from source to destination.

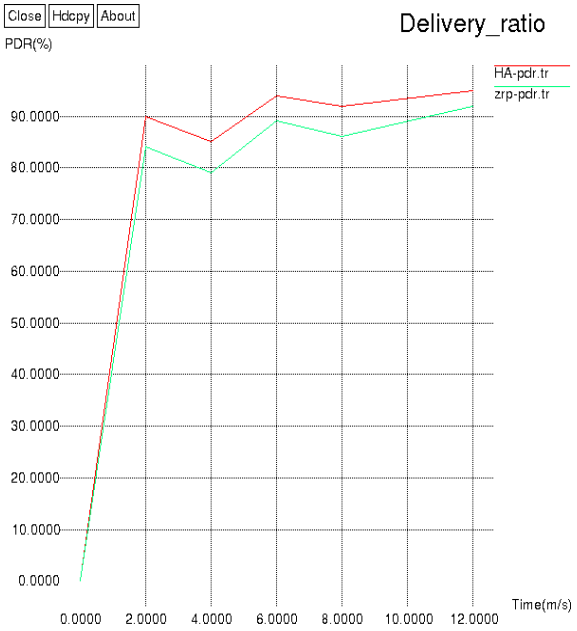

Fig 6. Delivery _ratio of ZRP Vs. ABEZRP

In Fig 6, ABE-ZRP depicts the ratio of delivery improvement at higher ranges of Packet size compared with evaluated ZRP values shown with a red spike for HA and a green spike for ZRP.

C. Overall Evaluation of QoS Parameters

Table 2. Comparison of Performance factors

PERFORMANCE PARAMETERS	ZRP	ABE-ZRP
THROUGHPUT	82%	96%
LOAD BALANCING	71%	96%
ENERGY CONSUMPTION	95%	36%
END TO END DELAY	99%	73%
DELIVERY RATIO	95%	99%

Table 2 reflects the gradual improvement in quality factors at a noticeable pace between the existing and proposed systems with enhanced security features piggybacking data transmission in an Ad hoc network.

VI. CONCLUSION

The contribution of this research is to propose a methodology for enhanced energy efficiency and security in ZRP. Our focus is mainly on the security aspects like confidentiality with authentication of data at nodes and establishing an optimized routing path considering node lifetime. ABE Encryption infusion with Diffie Hellman is used for ensuring secured data transfer between nodes. Data transfer is initiated by exchanging keys between source and destination. The computed results of the hybrid approach reflect an enhanced performance in comparison with ZRP. By this technique, malicious nodes cannot affect the network's performance, and data can be transmitted in the safest path. The ABE technique can be used in other protocols merging with different efficient cryptographic algorithms could bring out a finer and secure algorithm in the future.

VII. REFERENCES

[1] Moudni, H., Er-rouidi, M., Mouncif, H., & Hadadi, B. E. (2016). Secure routing protocols for mobile ad hoc networks.International Conference on Information Technology for Organizations Development(IT4OD). DOI:10.1109/it4od.2016.747929,(1-6)(2016). IEEE. https://ieeexplore.ieee.org/document/7479295.

[2] A. Subramaniam, Power management in zone routing protocol (ZRP), University of Central England, Birmingham,(2003).

[3] Sharma, S., Jain, A., & Gupta, N. Modified ZRP to Identify Cooperative Attacks. 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT). (2016),DOI:10.1109/cict.2016.66,(302-307)IEEE. https://ieeexplore.ieee.org/document/7546620/

[4] Mehta, D., Kashyap, I., & Zafar, S. Random cluster head selection based routing approach for energy enrichment in MANET. 2017 International Conference on Recent Innovations in Signal

Processing and Embedded Systems (RISE). DOI:10.1109/rise.2017.8378137,IEEE, (2017).

[5] Barolli, L., Honma, Y., Koyama, A., Durresi, A., & Arai, J. (2004). A selective border-casting zone routing protocol for ad-hoc networks. Proceedings. 15th International Workshop on Database and Expert SystemsApplications,(2004). DOI:10.1109/dexa.2004.1333494 (pp 326-330) IEEE. https://ieeexplore.ieee.org/document/1333494/.

[6] Pham Thi Minh, T., Nguyen, T. T., & Kim, D.-S. (2015). Location Aided Zone Routing Protocol in Mobile Ad Hoc Networks. IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA).(2015).DOI:10.1109/etfa.2015.7301615 https://ieeexplore.ieee.org/document/7301615.

[7] Chellathurai, A. S., & Darma Prakash Raj, E. G. (2013). EZRP: Evolutionary Zone Routing Protocol. 2013 International Conference on Advanced Computing and Communication Systems. DOI:10.1109/icaccs.2013.6938740,(1-5)IEEE. https://ieeexplore.ieee.org/document/6938740

[8] Malwe, S. R., Rohilla, S., & Biswas, G. P. Location and selective-border cast based enhancement of the zone routing protocol. 2016 3rd International Conference on Recent Advances in Information Technology (RAIT). DOI:10.1109/rait.2016.7507880 (2016) 8388.IEEE.https://ieeexplore.ieee.org/document/7507880.

[9] Osama A. Awad, Mariam Rushd, An Efficient Energy-Aware ZRP-Fuzzy Clustering Protocol for WSN, International Journal of Scientific & Engineering Research, 7(3)(2016) 1060-63, ISSN 2229-5518.doi:10.13140/RG.2.1.3738.9205. https://www.researchgate.net/publication/301224008_An_Efficient_Energy_Aware_ZRP-Fuzzy_Clustering_Protocol_for_WSN.

[10] Varun Kumar Sharma, Lal Pratap Verma, and Mahesh Kumar, A Fuzzy-based Adaptive Energy Efficient Load Distribution Scheme in Ad-hoc Networks, I.J. Intelligent Systems, and Applications,2(2018) 72-84, DOI:10.5815/ijisa.2018.02.07 https://www.researchgate.net/publication/322909008_A_Fuzzy-based_Adaptive_Energy_Efficient_Load_Distribution_Scheme_in_Ad-hoc_Networks .

[11] Hossain, S., Hussain, M. S., Ema, R. R., Dutta, S., Sarkar, S., & Islam, T. (2019). Detecting Blackhole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET. (2019),10th International Conference on Computing, Communication, and Networking Technologies(ICCCNT). DOI: 10.1109/ICCCNT45670.2019.8944395. https://ieeexplore.ieee.org/abstract/document/8944395.

[12] K.Spurthi, T.N.Shankar, A Research on Wormhole Attack in Mobile Adhoc Networks, International Journal Of Recent Technology and Engineering,8(14) (2019) 1125-1130. https://www.ijrte.org/wp-content/uploads/papers/v8i1s4/A12130681S419.pdf.

[13] K.Spurthi, T.N.shankar, Intrusion Detection in Manets with Elgamal Digital Signature, Far East Journal of Electronics and communications,16(3)(2016) 511-525. https://www.researchgate.net/publication/308271411_Intrusion_detection_system_in_manets_with_elgamal_digital_signature.

[14] K.Spurthi, T.N.shankar, An Efficient Cluster Computing Mechanism for Wormhole Attack Detection in MANET, International Journal of Advanced Science and Technology 29(7)(2020) 3320-3333. http://sersc.org/journals/index.php/IJAST/article/view/18963.

[15] Rajinder Singh, Parvinder Singh, and Manoj Duhan, An Effective Implementation Of Security-Based Algorithmic Approach In Mobile Adhoc Networks, Human-Centric Computing And Information Sciences, Springerjournal.4(1),1-14,(2014). https://link.springer.com/article/10.1186/s13673-014-0007-9.

[16] Prakash, S., & Swaroop, A., A brief survey of black hole detection and avoidance for ZRP protocol in MANETs. 2016 International Conference on Computing, Communication, and Automation (ICCCA).(2016) DOI:10.1109/ccaa.2016.7813802 ,cross reference(https://ieeexplore.ieee.org/document/7813802)

[17] Sethi, K., Pradhan, A., Punith, R., & Bera, P. A Scalable Attribute-Based Encryption for Secure Data Storage and Access in Cloud. 2019 International Conference on Cyber Security and Protection of Digital Services(CyberSecurity). (2019).DOI:10.1109/cybersecpods.2019.8884981(https://ieeexplore.ieee.org/document/8884981).

[18] Nan Li. Research on Diffie-Hellman key exchange protocol. 2010 2nd International Conference on Computer Engineering and Technology. (2010). DOI:10.1109/iccet.2010.5485276 (https://ieeexplore.ieee.org/document/5485276).

[19] Alinci, M., Spaho, E., Lala, A., & Kolici, V., Clustering Algorithms in MANETs: A Review. 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems. (2015) .DOI:10.1109/cisis.2015.47(https://ieeexplore.ieee.org/document/7185207).

[20] Mehta, S., Sharma, P., & Kotecha, K., A survey on various cluster head election algorithms for MANET. 2011 Nirma University International Conference on Engineering. (2011).DOI:10.1109/nuicone.2011.6153248 (https://ieeexplore.ieee.org/document/6153248).

[21] XueqinYanga, QiangweiChen, bChaoboChen, bJianhuaZhaob, Improved ZRP Routing Protocol Based on Clustering procedia computer science, 131,992-1000, (2018).https://doi.org/10.1016/j.procs.2018.04.242 .

[22] Rajput, S. S., & Trivedi, M. C., Securing Zone Routing Protocol in MANET Using Authentication Technique. 2014 International Conference on Computational Intelligence and Communication Networks.(2014),DOI:10.1109/cicn.2014.184 (https://ieeexplore.ieee.org/abstract/document/7065604).