Journal of Scientific & Industrial Research
Vol. 81, January 2022, pp. 69-75

Hybrid Energy Efficient Secured Attribute based ZRP Aiding Authentic Data Transmission

Kollu Spurthi* and T N Shankar
[1]Dept of CSE, KLEF, Guntur, 522 502 Andhar Pradesh, India

Received 05 January 2021; revised 18 December 2021; accepted 26 December 2021

The modern furtherance in mobile Ad-hoc networks with evolving technology is challenging the researcher's calibre in several aspects concerning routing MANETS with dynamic structure rely on the routing factor for reliable transmission. Routing protocols dictate the performance of networks in Wireless environments. Practitioner's research introduces routing protocols falling into categories like Proactive, Reactive and Hybrid routing protocols. Zone Routing Protocol (ZRP), a multicast routing protocol is gaining attention as it fusions the features of both proactive and Reactive protocols. Our work addresses the energy consumption issues and security breaches in the routing process of ZRP, thereby furnishing with a Hybrid Approach. The proposed Model leverages transmission efficiency by periodically reducing the number of unwanted nodes consuming energy and providing additional security instances using ABE-based encryption. Various Qualities of Service (QoS) parameters like throughput, end-to-end delay (E2ED), load balancing, energy consumption, and delivery ratio have shown that the hybrid technique is effective compared to the traditional ZRP.

Keywords: Attribute based encryption, Energy, MANET, Network security, QoS Parameters

Introduction

Despite their contributions to Ad-hoc networks, numerous researches left a few issues unaddressed, enabling more advancement and research in this area, because it is dynamically customizing by nature. MANETS an unsupervised network, is vulnerable to attacks and should rely on Routing as its primary function. Innumerable protocols, classified as Proactive, Reactive, and Hybrid have been emerged from the Literature Legacy Studies. Ad-hoc wireless networks, like MANETs, deny the validity of a fixed infrastructure. They've been a part of the research community since the mid-1990s, and they've continued to grow, encompassing a wide range of issues such as routing security, transmission medium, and more. A network's ability to adapt to changing topologies due to the mobility of its nodes makes it a popular choice in wireless environments. This form of the network allows devices to join and depart at any time.

The ability of this network to respond to various conditions is reflected in defence networks that enable hopping mines, which appear and disappear as a mission comes to an end. Additionally, the military, disaster management, data mining, and espionage on IoT[1] based smart homes are just some of the additional uses. These technologies rely on a single key for sending data between nodes. An important topic in data transport and routing has impacted the field of study. A wired or wireless network must include a central feature known as routing that show different characteristics depending on the network conditions. Researchers are under pressure to come up with new protocols for wireless networks, which are constantly changing their configurations and changing their nodes across.

For the last few years, researchers have focussed on how to avoid a survey. Solution oriented, reactive and hybrid methods have developed as a result of this process. Table-driven and on-demand protocols are the alias names for proactive and reactive, respectively. This type of table-driven protocol periodically exchanges and distributes the routing tables to maintain a current list of targeted nodes and their associated routes. These reactive techniques enable rapid route identification and reliability at a high cost, but they also delay the response time for restoration and failures. In this category, there are algorithms such as DSDV, OLSR, and WRP. A reactive protocol's foundation is responding to requests on time, such as AOMDV, DSR, and TORA.

*Author for Correspondence
E-mail: Kolluspoorthy03@gmail.com

To investigate ZRP, CEDAR, and FSR under the hybrid category includes ZRP in our research. MANETs are getting popular because of their efficiency and simplicity in real-time applications. However, the performance of MANET is hindered by its QoS factors, such as bandwidth, reduced packet loss, transmission delay, and security thumbnails, to name a few.[2] It is difficult to implement QoS in MANETs because of the network's inherent characteristics, including a lack of centralized infrastructure, resources, inconsistent location, and more incredible energy requirement.[3]

The Hybrid ABE—ZRP framework provides authentication services through a secure transmission network with less energy consumption. This work aims to focus on lowered energy consumption in ZRP and secured transmission of routing information for reliable communication. The QoS variables such as energy efficiency, throughput, end to end delay, load balancing and security concerns are better regulated by the recommended hybrid routing protocol.

Zone Routing Protocol

The Zone Routing Protocol (ZRP) emerged as a hybrid framework, where nodes maintain routes to respective destinations lying within and between zones. Here, the dynamic face of control takes charge with current routing information if the packet needs to be transported within zone.[4] The protocol's reactive nature kicks in when the package is about to cross the premises, ensuring that it gets to its intended destination within the boundaries of the structure. ZRP concludes by nature of its destination as mentioned above into IARP and IERP.[5]

The IARP targets service within the zone[6] as the routing table undergoes continuous changes based on triggered connectivity of neighbouring nodes. Once the neighbour is identified, a replica of the new routing table is shared with its new peers. Update received is instantly reflected in their routing tables. The nodes which are within the predefined radius[7] will become the participant nodes to receive the updates. The measuring unit for a confined radius differs based on the considerations like hop counts or distance between the nodes and so on.

IERP protocol rises when the target node is located outside the routing zone, and a path needs to be laid. It makes use of the query response concept to uncover paths when demanded. Differentiation of IERP from other pre-existing algorithms relying on flooding by exploring routing zones structures with border warriors who lay route to other zones. This mechanism is named as Border Casting. Border Casting, as named casts the packets distinctly only to peripheral nodes by relay transferring them to border bypassing the non-peripheral nodes from intercepting. This Broadcast Resolution protocol performs its service by receiving information from IARP and flushes it outside the zone for identifying the destination path by multicasting. In this transfer, if the destination node is attained in that zone, an acknowledge message is traversed back to the source else the packet is assigned to the peripheral nodes of the received zone These peripheral nodes repeat this task with is neighbouring nodes until the destination is acquired via borders of routing zone with the technique termed Broadcasting.

Even though energy efficiency is not a mark able trade-off in ZRP[8], still work for optimal energy consumption is studied for literature and focused on maximizing performance.[9] Despite a strong framework on which ZRP is built and several remarkable protocols holding the pride of ZRP, few factors that are directly or indirectly decorating the performance namely the security aspects and considerable energy consumption.

Parameters of Interest

Parameters considered for analysis and improvement in our work are restricted to energy consumption by nodes in Ad-hoc network using zone routing protocol and security concerns during information sharing.

The influencing parameters of energy efficiency which may be subjected to optimization[10] are node count improvement, connection count, discrete speeds, fluctuating data rates, and enhancing network lifetime.

Security factor influences the performance of routing protocols and have a higher risk of pulling down the network quality. A wide variety of attacks can disrupt communication between source and destination nodes by preventing data transmission between them. In addition, there are a number of other examples of these types of attacks such as the Sinkhole attack, the Wormhole assault, the Black-hole assault etc.[11]

Sinkhole attack works by attacking data nodes, identifying source and destination information, these after fake requests, and generating illegal paths by authenticating using sequence numbers. This attack degrades the performance of the network by taking over control on transmission and even encourages packet dropping overhead.

Wormhole attack by its virtue asserts the illusion of short path availability than the original one. Wormhole takes the help of malicious nodes, henceforth creating tunnel which is rich in information dropping, link failures, disrupting data and routing, etc. finally ending up in a loss of performance.

Black hole is a well-known simple and effective attack that is defined based on its capabilities of inserting a malicious node. This node is well versed at attaining the identity of valid nodes on the ADHOC network as then is no physical restriction.[12] Such insertion brings about disturbances within the network provoking an attack to drape the packets and to cut the communication by forwarding to a non-existent node.

A Grey hole attack is also termed as a packet drop attack. This attack advertises a false route deceiving legitimate node to lay a route via malicious[13] node. This node responds to route requests with route reply and sends false information which makes legal nodes assume that the route to the destination through grey whole node is legitimate. This attack targets the packet drop.

The DDOS is a multi-scale attack by malicious users via flooding the chosen network with innumerable[14] packets. This flooding leads to the collapse of the victim by running out of its resources like computing ability, bandwidth, etc. This forces the network to be incapable of serving the legal clients due to the infinite number of flooded unwanted packets.

The attacks mentioned above ping the routing of MANETs resulting in network degradation and failures. MANETs will respond to future attacks by employing advanced routing protocols and encryption standards, among which ZRP is our preferred choice for our evaluation. In conjunction with Diffie-Hellman, ABE is selected as additional parameter for improving security.

Asymmetric encryption, known as ABE, utilizes a pair of public[15] and private keys. Properties of nodes are used to transform plain text into encrypted messages and vice versa based on the secret key used by the sender and receiver. As a result, security elements like authentication, access control, integrity and confidentially can all be provided by encryption. The ability of ABE to endure collisions with two ABE Schemes is a critical security feature.[16] The Diffie-Hellman key exchange is a vital component of our policy-based ABE. As part of the ABE algorithm, Diffie-Hellman key exchange is used to extract the Public and Private Key pairs that are opted to protect during data exchange. As a result of the Diffie-Hellman algorithm designed by the National Security Agency, the two parties can agree on terms that allow secured communication across a public network using an alternative encryption technique of their selection.

Proposed Framework

Though ZRP continues to be an efficient hybrid routing protocol, few parameters like energy consumption and security inject adverse effects thereby degrading the performance. To handle these consequences, we contribute a hybrid approach which enhances energy utilization by clustering and fuzzy classification of nodes using delay mechanism. Additionally, our technique successfully resolves the security threats and attacks using attribute-based encryption in combination with Diffie hellmen key exchange.

The Approach's three key phases are Cluster Head Selection, Security Phase, and Performance evaluation.

Cluster Head Selection

The network is divided into clusters and nodes internally share routing information. When the packets are routed to destinations beyond boundaries of a network zone, the BRP takes over the transmission. Here the packet is transferred to the peripheral border nodes for being transmitted to other zones. This is handled by the border routing protocol using RREQ packets targeting only peripheral nodes. Distance and energy of each node in the cluster is calculated for predefined threshold time for selecting the cluster head. Distance and energy are computed as

$$\text{Avg\_distance} = \frac{\sum_{i=1}^{n} d}{n}$$

let n be the no. of nodes, d be the distance measure from node — all the nodes in zone(region)

$$E = E_{tx} + E_{rx}$$

$$E_{tx} = E_{dis} * L + E_{traA} * L * d^2$$

$$E_{rx} = E_{dis} * L$$

Energy consumption is calculated by sum of the energy consumed for data transmission (E_{tx}) and receiving data packets (E_{rx}) where E_{dis} is the energy dissipation, E_{traA} is the transmitted energy for amplifier, L is the no. of bits ranging between 1 to128 bits, d is the distance between nodes.

Security enhancement

During exchange of routing information, chances of nodes being prone to attacks increase. To handle the consequences and provide secure and reliable transmission attribute-based encryption is considered. In ABE node properties like node location, bit rate, packet sizes are taken for computation and evaluation of secret key. The generated secret key is shared securely using Diffie hellmen key exchange and these secret keys keep varying at regular intervals of time. The secret key generation for nodes x, y is formulated as follows.

$$f(x, y) = \sum_{i,j=0} q_{ij} x^{i} y^{j}, where(q_{ij} = q_{ji})$$

where q is large prime number, i is the cryptographic key and j is the common key, with i, j values ranging between 0 and n.

Transfer of routing information results in the dropping of energy levels at nodes. These energy levels are recomputed to check whether they fall between the ranges of predefined sensitivities. Nodes in the zone are classified using fuzzy classification into 3 groups based on their retained energy levels as Safety phase, Risky phase, and High-risk phase. Among them the high-risk phase nodes are subjected to avoidance of overhearing thereby compelling such nodes to sleep, nodes in the safety phase participate in data transmission. Here every node holds the packet for a predefined time limit that is inversely proportional to energy level of that node by opting delay function.

$$Delay = del\ (n) + \left({}^{5}/_{(e + 5)}\right)$$

where del (n) is delay bit for each node (i.e. minimum delay at each station) and e is the energy of the node.

MANET's, suffering from several adhesive attacks discussed are centric around malicious nodes being embedded into the network. To fight back this inception of malicious nodes into a network, ABE, encryption is opted as it is characterized around attributes about a transmission entity and withstands a network being collapsed.

Performance Evaluation and Analysis

The Proposed hybrid approach is implemented with network simulator NS3.2 is an event driven simulation tool that offers advantages in learning the dynamic nature of nodes in networks. Several network protocols are well simulated using this tool. The version opted for our simulation offers a modular library support instancing simulation models there by allowing external routing. The parameters considered for assigned with initial values are initialized as shown in Table 1 with 36 nodes taken for consideration holding 1 joule energy when the simulation process initiates with execution time of 120 seconds. The efficiency of proposed ABE-ZRP Technique is compared against conventional ZRP using matrices considered as throughput, Load-Balancing, Energy-consumption, End-to-End Delay, and Delivery-ratio. Performance of the model reflects the leveraged delivery of packets within the considered time strip. Higher the Performance more the efficiency and intended throughput.

$$\text{Throughput} = \frac{\text{Total number of packets delivered}}{\text{Time}}$$

The time dissipated during transmission with delays defines the End to end delay and demands for a lower value for enhanced performance.

$$\text{End to end Deivery (E)} = \text{B} \times {}^{\text{L}}/_{\text{T}}$$

where, B — no. of bits, L — no. of links and T—Transmission rate.

The proportion of the packets transmitted via network and packets reached at destination host defines Packet Delivery Ratio, which promises a higher performance with improved values of packet delivery.

$$\text{PDR} = \frac{\text{Numberof packets delivered}}{\text{Total number of packets sent}}$$

The proposed approach is compared with IZRP, LEACH and the outcome of improved throughput is depicted in Fig. 1 with a red spike on the scale of X graph for our proposed Hybrid Approach designated HA and green spike for ZRP.

In Fig. 2 we successfully project reduced Energy consumption by our proposed model.

Table 1 — Simulation Parameters

PARAMETERS	VALUES
Simulator	NS2
Simulator Time	3.40000 s
Simulation Area	1000*1000 m
Proposed Protocol	hybrid approach
Energy of nodes	2 Joules
Nodes considered	34
Bit Rate	1Mb/sec
Packet Length	600 bytes

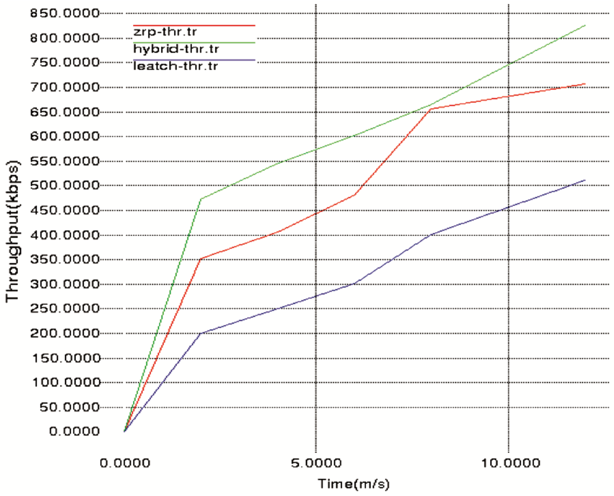


Fig. 1 — Comparison of Throughput

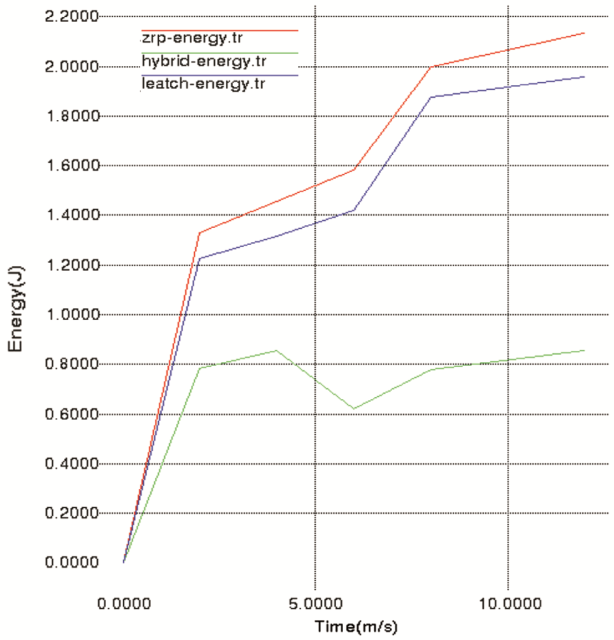


Fig. 2 — Comparison of Energy Consumption

In Fig. 3 our proposed model HA shows a substantial reduction in End to End delay with a green spike for proposed hybrid model, when compared with a red spike representing IZRP and Leach, exhibiting a longer delay during transmission from source to destination.

Finally in Fig. 4 the delivery improvement ratio for high range packet size in comparison is depicted when evaluated against ZRP values shown with a red spike for HA and green spike for IZRP.

In Fig. 5 our proposed model HA shows simulation of 36 nodes using NS3.2 and clearly elicits the clustering of nodes using ZRP routing protocol.

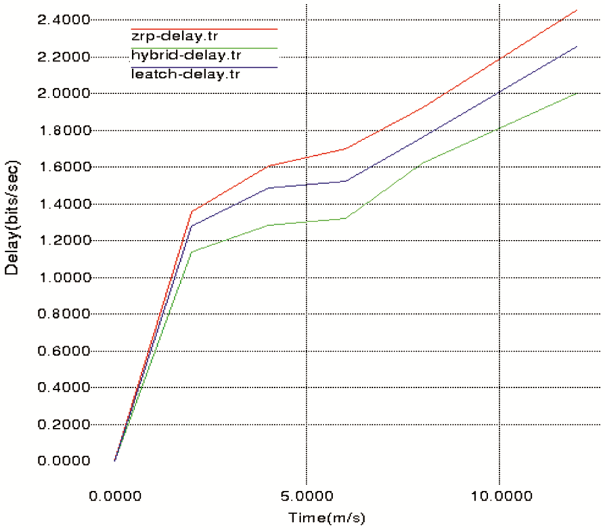


Fig. 3 — Comparison of E2E Delay

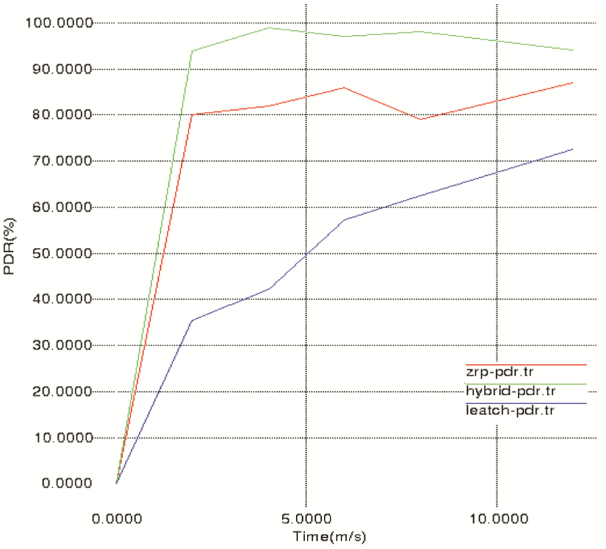
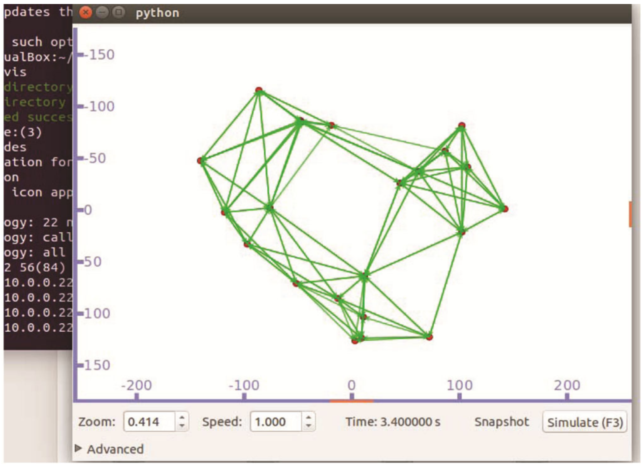


Fig. 4 — Comparison of Delivery _ratio



```
pdates th

 such opt
ualBox:~/
vis
directory
irectory
ed succes
e:(3)
des
ation for
on
 icon app

ogy: 22 n
ogy: call
ogy: all
2 56(84)
10.0.0.22
10.0.0.22
10.0.0.22
10.0.0.22
```

Fig. 5 — showing nodes simulation

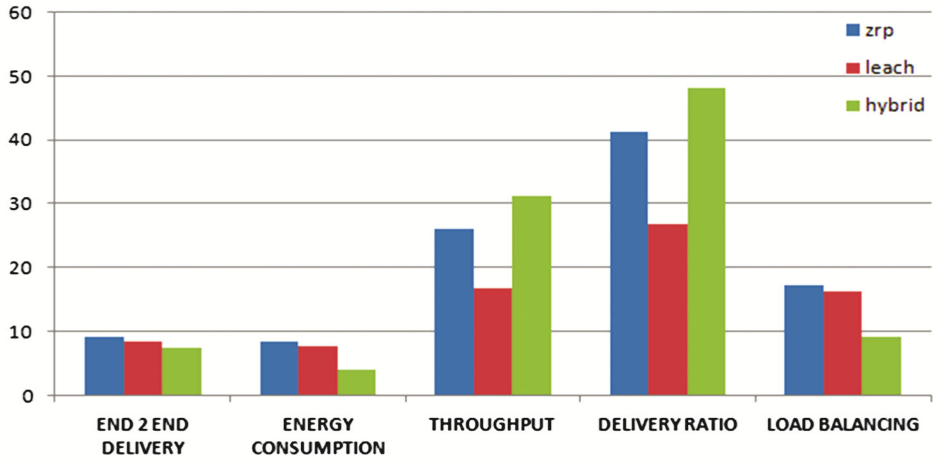


Fig. 6 — Comparison of Performance factors

The data in Table 1 can be used for overall evaluation of QoS Parameters and Fig. 6 reflects a summarized enhancement in quality factors with considerable raise between the existing and proposed systems with enhanced security features the transmission of data in an Ad hoc network.

Conclusions

The proposed approach successfully contributes in enhancing energy efficiency and this tag to be a concerning factor affecting the overall performance in Ad-hoc networks. The nodes falling in high-risk edge of a zone based on fore mentioned conditions implicitly enter into a sleep state adding to reduced energy consumption by the channel. This decrease in energy factor owes to be an awaiting urge for leveraged network throughput. Security aspects arising from lack of confidentiality and authentication are also focussed and resolved in the work using Attribute Based Encryption. To ensure reliable and secure communication between nodes, ABE considers features that rely on the secret key derived from sensitive attributes of node location in the network. It works in infusion with Diffie Hellman to initiate exchange of public and private keys among source and destination for addressing authentication problem knocking out the attempt of malicious nodes. The computed results of the hybrid approach override the traditional ZRP in all the QoS factors[17] considered. Adding to future scope, Various Cryptographic techniques can be imposed on Routing protocols to enhance the security and improve few quality factors which are worth appreciating the advantages of MANET's.

References

1 Gasmi R, Aliouat M & Seba H, A stable link based zone routing protocol (SL-ZRP) for internet of vehicles environment, *Wirel Pers Commun*, (2020), doi:10.1007/s11277-020-07090-y.

2 Liu J, Xu Y & Li Z, Resource allocation for performance enhancement in mobile Ad-hoc networks, *IEEE Access*, (2019) 1–1, doi:10.1109/access.2019.2921075.

3 Ravi G & Kashwan K R, A new routing protocol for energy efficient mobile applications for ad hoc networks, *Comput Electr Eng*, **48** (2015) 77–85, doi:10.1016/j.compeleceng.2015.03.023.

4 Khudayer B H, Anbar M, Hanshi S M & Wan T C, Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks, *IEEE Access*, (2020) 1–1, doi:10.1109/access.2020.2970279.

5 Ravilla D & Putta C S R, Energy management in zone routing protocol (ZRP), *Advs Comp Sci Eng Appl*, (2012) 355–366, doi:10.1007/978-3-642-30111-7_34.

6 Mohandas R, Krishnamoorthi K & Sudha V, Energy sensitive cluster level security selection scheme for MANET, *Wirel Pers Commun*, (2019), doi:10.1007/s11277-019-06131-5.

7 Sudarsan D, Mahalingam P R & Jisha G, Distance aware zone routing protocol for less delay transmission and efficient bandwidth utilization, *Advs Comp Sci Eng Appl*, (2012) 63–71, doi:10.1007/978-3-642-30111-7_7.

8 Kuo W K & Chu S H, Energy efficiency optimization for mobile ad hoc networks, *IEEE Access*, **4** (2016) 928–940, doi:10.1109/access.2016.2538269.

9 Awad O A & Rushd M, An efficient energy-aware ZRP-fuzzy clustering protocol for WSN, *Int J Eng Res*, **7(3)** (2016) 1060–1063.

10 Sharma V K, Verma L P & Kumar M, A Fuzzy-based adaptive energy efficient load distribution scheme in Ad-hoc networks, *Int J Intell Syst Appl*, **2** (2018) 72–84, doi : 10.5815/ijisa.2018.02.07.

11 Singh R, Singh P & Duhan M, An effective implementation of security-based algorithmic approach in mobile Ad-hoc networks, *Hum—centric comput inf sci*, **4(1)** (2014) 1–14.

12 Hawbani A, Wang X, Abudukelimu A, Kuhlani H, Qarariyah A & Ghannami A, Zone probabilistic routing for wireless sensor networks, *IEEE Trans Mob Comput*, (2018) 1–1, doi:10.1109/tmc.2018.2839746.

13 Jamal T & Butt S A, Malicious node analysis in MANETS, *Int J Inf Technol*, 2018, doi:10.1007/s41870-018-0168-2.

14 Anbarasan M, Prakash S, Antonidoss A & Anand M, Improved encryption protocol for secure communication in trusted MANETs against denial of service attack, *Multimed Tools Appl*, (2018), doi:10.1007/s11042-018-6777-8.

15 Yang Y, Chen X, Chen H, & Du X, Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing, *IEEE Access*, **6** (2018) 18009–18021, doi:10.1109/access.2018.2820182.

16 Song Y, Wang H, Wei X & Wu L, Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud, *Secur Commun Netw*, 1–9, (2019), doi:10.1155/2019/3249726.

17 Spurthi K & Shankar T N, An improved zone routing protocol for secure and efficient energy management, *Int J Eng Trends* Appl, **69(1)** (2021) 29–34.