

Optimized image processing and clustering to mitigate security threats in mobile ad hoc network

Ibrahim A. Alameri¹, Jawad kadhim mutar², Ameer N. Onaizah³, Iftikhar Ahmed Koondhar⁴

¹Jaber ibn Hayyan Medical University, Iraq

¹University of Pardubice, Faculty of Economics and Administration, Czech Republic

²College of Education for Humanity Sciences, Almathana University, Iraq

^{3,4}School of Computer Science and Technology, Beijing Institute of Technology, China

³University of Kufa, Iraq

Article Info

Article history:

Received Aug 16, 2019

Revised Dec 5, 2019

Accepted Dec 25, 2019

Keywords:

Image analysis

Image processing

MANET

Security

Weighted clustering algorithm

ABSTRACT

Since there are provisions of many attributes that are not possible or difficult to follow by networks conventionally, mobile ad-hoc networks are extensively deployed. This application starts through the defense sectors, the sensory node presents in the hostile territories down to the gadgets for congestion communication in traffic by general transportation when travelling for adequate provision of infrastructure during disaster recovery. As a lot of importance related to (mobile ad hoc network) MANET application, one important factor in ad-hoc networks is security. Using image processing for securing MANET is the area of focus of this research. Therefore, in this article, the security threats are assessed and representative proposals are summarized in ad-hoc network's context. The study reviewed the current situation of the art for original to security provision called mobile ad hoc network for wireless networking. The threats to security are recognized while the present solution is observed. The study additionally summarized education erudite, talks on general issues and future instructions are recognized. Also, in this study, the forecast weighted clustering algorithm (FWCA) is employed as a cluster head over weighted clustering algorithm (WCA) is examined as quality in cluster-based routing, service is highly significant with MANET.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ibrahim A. Alameri,

Jaber ibn Hayyan Medical University, Najaf, Iraq.

University of Pardubice, Pardubice, Czeck Republic.

Email: ib.alameri@jmu.edu.iq, ibrahim.alameri@student.upce.cz

1. INTRODUCTION

The The application of computer algorithm to carry out processing of image on digital images is called digital image processing (DIP) [1]. There are many advantages related to DIP as a field of digital dispensation or sub-category or analog image processing in excess. An effective deal is provided in broader algorithm range to be practiced to enter data with easy prevention of "evils" like: signal distortion and build-up noise. DIP may be developed in the form of multi-dimensional system since definitions of images are over two-dimensions or more. Images are classified based on their source such as x-ray and visual. The electromagnetic energy range is the principal source of energy for images; while other sources of energy are: electronic; ultrasonic and acoustic. The digital image is mapped and sampled as a picture elements or pixels or a grid of dots. Those digital images are electronically taken snapshots from scene or scanned documents like manuscripts, printed

works, photographs and artworks. While the computer generates the visualization, the synthetic images are used for modelling [2].

A total value such as white, black, shades of colour or grey that are assigned to each pixel is represented in binary codes as ones and zeros. A computer is used to store the bits or binary digit for each pixel in a sequence and it is usually called “compressed” as it is being represented mathematically. The computer read and then interpreted the bits to generate an account of analog to display [3]. The basic steps during the processing of digital image are: image acquisition, image enhancement, image restoration, colour image processing, processing of multi-resolution and wavelets, segmentation, description, recognition and representation of object and morphological processing. Analysis and processing of digital image are applied in industrial and educational application and in a wide range of artistic [4]. Processing and analysis of soft image is generally presented in all main platforms of computers. Environmental science, art, medicine and biotechnology all use image processing.

Therefore, this study proposed a novel method through which security can be provided in all phases. A trust based multipath routing protocol is used in order to enhance security in the routing phase. As intruders can monitor and intercept the password, thus, the authentication key transfer in MANET networks via nameless midway nodes is not suitable to be used. It is imperative to use a strong secure method of key transfer that hides data of verification keys. Therefore, in this article, the threats to security assess are assessed and representative proposals are summarized in ad-hoc network’s context. The study reviewed the current situation of the art for original to security provision called mobile ad hoc network for wireless networking.

2. LITERATURE REVIEW

2.1. Image processing

In a broadest term, an image processing is an umbrella term used for analysing and representing data in visual form [5]. It is regarded as the manipulation of numeric data present in a digital image in an attempt to enhance its visual appearance. Satellite photographs can be calibrated, medical images can be clarified and faded pictures can be enhanced through image processing. Numeric information can also be translated into visual images by image processing that can be edited, animated, filtered and enhanced in order to show the association previously not apparent [6]. Analysis of image involves collection of data from digital images in form of measurements that can be transformed and analysed. An accurate digital substitute for callipers and rulers is provided by the image analysis.

Images are classified in accordance with their source e.g. X-ray, visual and so on. The electromagnetic energy spectrum is the principal energy source for images. The ultrasonic, electronic and the acoustic are other sources of energy. While the visualization is generated by the computer, the synthetic images are used for modelling. Digital images are electronic snapshots taken from a scanned or scene of documents such as artwork, printed text, manuscripts and photographs [7]. The digital image is mapped and sampled as a grid of pixels, picture elements and dots. A tonal value is attached to each pixel i.e. white, black, shades of grey or color which is represented in binary code as zeros and ones. The binary digits or bits for each pixel are stored in a sequence by a computer and often minimized to a mathematical representation called compressed. The bits are then read and interpreted by the computer to produce an analog version for display or printing. In digital image processing, the fundamental steps include [8]:

- Acquisition of image
- Enhancement of image
- Restoration of image
- Processing of colour image
- Wavelets and multi-resolution processing
- Compression
- Morphological processing
- Segmentation
- Description and representation

2.2. Mobile Ad-Hoc networks

Cloud services can be accessed either by wired network or wireless [9, 10] however MANET is a wireless network where every device communicate wirelessly [11, 12]. A mobile ad-hoc network (MANET) is often distinguished as networks with many free and independent nodes, with mobile device composition and other related pieces of mobile, which place themselves in different categories of setups and the capacity of type of network, is still under research. MANET is becoming popular more due to its ease of deployment, flexibility and low cost. Meanwhile to the network must follow a protocol of sophisticated routing in order to achieve

these benefits. The protocols that were early proposed are not designed to operate when the attackers are present. Thus, this led to some major challenges in MANETs as explained in the Table 1 [13-20].

Table 1. Large-scale of challenges in MANETs

Challenges		Clarification
1	Independence	In managing different actions of nodes of mobile, there is no centralized management entity available
2	Dynamic topology	In a random manner, nodes can be connected and mobile dynamically. The connection of the networks is in variation timely and is in proximities to each other in additional nodes accordingly.
3	Device Detection	Identification of node relevancies in terms of moves and giving information on the need for existence of dynamic update lessen the difficulties in automatic selection of optimal route.
4	Bandwidth optimization	In terms of capacity, the wired links are greater than the wireless links.
5	Security	Susceptibility of the mobile link to both internal and external intrusion as render of mobility of node. A big challenge in MANET can be any node that can enter and leave freely the network and give security communication.
6	Topology Maintenance	One of the major threats among the MANET's nodes is the information updates of dynamic links.
7	Network Configuration	The fact that there is dynamism in the infrastructure of MANET is the motive behind the connection and disconnection of the variable links.
8	Limited Resources	As power and storage capacity are strictly partial, mobile nodes has a reliance on battery power – a very scarce resource.
9	Scalability	This is whether the network is able to make a provision in the presence of large numbers of nodes on an acceptable level of service.
10	Limitation in physical security	Mobility means high risk in security such as shared accessible wireless medium or peer to peer network agriculture to both malicious attackers and legitimate network users. There should be consideration for spoofing, service attack denial and eaves dropping
11	Infrastructure-less and self-operation	Manet is required by self-healing function in order to integrate into blanket of moving nodes out of range.
12	Poor Transmission of Quality	This is a wireless communication related problem as a result of many inherent source of error that lead to degradation of received signal
13	Ad Hoc Addressing	Problems related to implementation of standard addressing scheme

Assurance of MANET networks is the major challenge due to its susceptibility to attacks in a mobile link while the mobility of the nodes renders the network to possessing a highly dynamic topology. External and internal are the two categories of attacks against routing protocols. The internal attack is a result of a misconfigured, malicious router, faulty and compromised inside a network domain. A temporary network is formed by a collection of wireless mobile hosts which forms finally the network in ad-hoc without the need to include a stand alone infrastructure or centralized administration [6]. Self organization and self- configuring are the characteristics of the mobile multi-hop ad- hoc network where network structure is subjected to dynamic changes as a result of node mobility.

In these nodes, channels of random access are utilized by the nodes and thus be incorporated to participate friendly in the multi- hop forwarding. Working as hosts and routers is what nodes of the network do and thus transmitting data to or from other nodes in the network. Forwarding the packets in an appropriate way between the destination and from the source of mobile ad- hoc network requires locating a path by a routine procedure when infrastructure support is missing as seen in the case of wireless network or when destination mode is out of the range of a source node transmitting packet. The nodes in these networks use wireless channel of random access, manifesting it in a good manner to put themselves in multi hop forwarding as shown in Figure 1. The nodes of networks can be the hosts and the routers data to or from other nodes in network.

Base station can reach all the mobile nodes within a cell with no routing using broadcast in a common wireless network. Taking ad hoc networks as example, data can be forwarded by each node to others. By the way, more challenges will be faced regarding dynamics topology which is known as unpredictable changes in connectivity. In the current work a novel method have been applied to achieve security in both phases. First to enhance security in the routing phase by use a trust based multipath routings. Secondly, discover a secured trustworthy path from a source to a destination with minimal overhead. In previous studies Multiple node disjoint paths are discovered to enhance the security of the data delivery phase. Furthermore, misbehaving nodes are detected and exempted from such paths using the trust value of the nodes It's well known that Sending confidential data on one path helps attackers to get the whole data easily, whereas sending it in parts on different disjointed paths increases the confidentiality robustness, as it is almost impossible to obtain all the parts of a message fragmented and sent on multiple paths existing between the source and the destination.

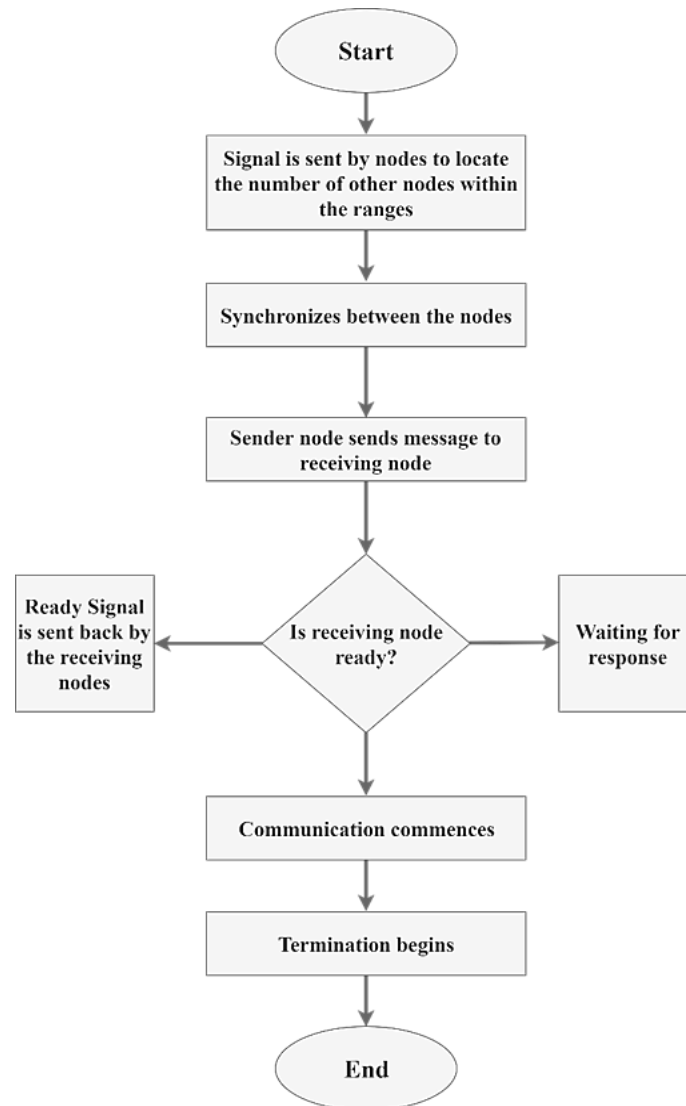


Figure 1. Network of a general ad-hoc in-action condition

2.3. System in existence

MANET has been made a popular topic of research with the growth of laptop system and Wi-Fi networking since the mid-1990s. Evaluations of different security measures are done by majority of academic papers for providing security against threat to MANET; most protocols are designed to provide security [21, 22]. Their capabilities are usually connected with all nodes within a few hops of one another assuming there are varying degrees of mobility within bounded space. Then, there is evaluation of different protocols according to the measure such as the packet drop rate, the end-to-end delays, the overhead introduced by routing protocol and network throughput [23-24].

In order to make password memorable and more secure, graphical passwords are introduced. By using graphical password, rather than typing alphanumeric characters, the users click on the images. The Pass Points are new graphical password system and more secure [25]. By digital watermark, authentication of image can be done [26]. A watermark can be used as a secret image or code encoded into an original image that its function is to identify both content and image owner. One of the forms of image authentication is the perpetual use of invisible watermarks. The algorithm of watermark is divided into three categories: marking algorithm; verification algorithm; and watermark.

The security of the system is improved by the approach of Déjà vu that depends not on recall-based authentication but on recognition-based. Through the ability to recognize previously seen images, the Déjà vu authenticates a user [2]. Using image processing and visual cryptography in Secure Authentication is an algorithm based on image processing and visual cryptography. This applies a way of customer signature processing and incorporating it into shares subsequently. The bank chose a scheme that determines the total

number of shares to be produced. Thus, during the creation of two shares, while one is kept by the customer, the other is stored in the bank of database. During all the deals of the customer, the share is presented. To get the original signature, the first share is stacked by this share. Therefore, decision is taken using correlation method whether rejection or acceptance of the customer and output authentication.

3. THE PROPOSED SYSTEM: SECURITY USING IMAGE PROCESSING FOR MANET

In Anytime there is entrance for a user into the mobile ad-hoc network in the nearest future, an image taken from a user is divided into two: the grey image of the original image of the user will be the first one and the file with image's colour pixel value is the other one. The part of the key shall comprise both the image and the file. There is encryption of the file and grey image with the aid of two keys of various types. The smallest size of the key in amount will have 128 bits. Then, the encrypted files will be joined and separated into smaller packets while with the aid from another key, each packet will be encrypted. Before the image processing, there are two layers of security from this way. Each packet passes via the network. After receiving packet at the side of handset with the support of first private, there will be separation of encrypted file for color pixel and. grey image values. After that, there will be decryption with the help of both files and this will join together to form the image. Small packet size for transmission must always be fixed from this proposed system to manage a better performance and the receiver side buffer space should be extended to avoid congestion. This complete image processing is supported under User Datagram Protocol (UDP) which has higher speed. Nodes When the network is being entered by the user and ready to transfer the secure data with other nodes in MANET:

- At first, the user captures or selects the input image and then selects the key meant for transmission.
- The user divides the key into two-half.
- The input colour image is divided by the user into: grey images with 256 grey levels and other with the text files are made up of components of RGB of the colour image.
- Addition of the divided key into grey and text image respectively.
- Then, the encryption of the grey and text image by applying one-time hash algorithm of cryptography.
- Followed by a separate transmission of grey image and text file into the network. This implies if an intruder gets a file, it would be hard to get a key due to the absence of the FULL key.
- After a separate decryption of the GREY image, by the combination RGB image TEXT files and the grey, the original image is constructed back.
- Lastly, there is combination of keys in order to have a secure key.

4. RESULTS OF THE EXPERIMENT

The process of taking the head of weighted clustering algorithm is accomplished by the instantaneous value of weight [24]. The reason why no eligible node can send its weight value because of the possibility of high traffic, although some nodes are able is to be a cluster head. This leads to the conclusion that the wrong selection of a cluster head can be taken place [25-27]. Accordingly, a solution for such an issue can be provided; it is FWCA (Forecast Weight Cluster Algorithm) this alternative takes the old value on a different side from the current value of the node. The result here leads to an appropriate head of a cluster. In order to calculate the forecast weight, a mode of computation is employed. This mode is called EMA: exponential moving average. This is useful in that it does not require the former values of forecast. [20, 28-30]. Forecasted weight (FW) is defined as:

$$FW = \alpha W_{\text{current}} + (1 - \alpha)FW_{\text{previous}} \quad (1)$$

α is a smoothing factor; a tunable parameter between zero and one. WCA can be used to calculate the weight of each node as:

$$Wi = w1di + w2Di + w3Si + w4Pi \quad (2)$$

where:

d = degree of difference in each node

D = Sum of distance with all neighbours

S = the node's speed

P = Battery consumed by the battery

$w1 + w2 + w3 + w4 = 1$.

The forecast weight (FW) is calculated in our proposed FWCA as:

$$FWi(t + 1) = a \sum_{k=0}^{t-1} (1 - a)^k FWi(t - k) + (1 - a)tWi \tag{3}$$

$FWi(t+1)$ = Forecast value for period $t + 1$ at time, t .

Wi = the actual value at period, t .

$FWi(t-k)$ = Forecast value for period t at time, $t - 1$

In Figure 2, there are several clusters, s_1, s_2, s_3 respectively at the server nodes of cluster 1, cluster 2 and cluster 3. The forecast weight is calculated with these nodes using weight value of nodes and the game theory approach is used to decide the cluster head to avoid confliction of having similar weights.

$$w1 + w2 + w3 + w4 = 1$$

$$w1 = 0.7$$

$$w1 = 0.2$$

$$w1 = 0.06.$$

Using the following formula, Tables 2, 3 and 4 [30] present the weight values of nodes for each cluster to calculate the weight:

$$Wi = w1di + w2Di + w3Si + w4Pi \tag{4}$$

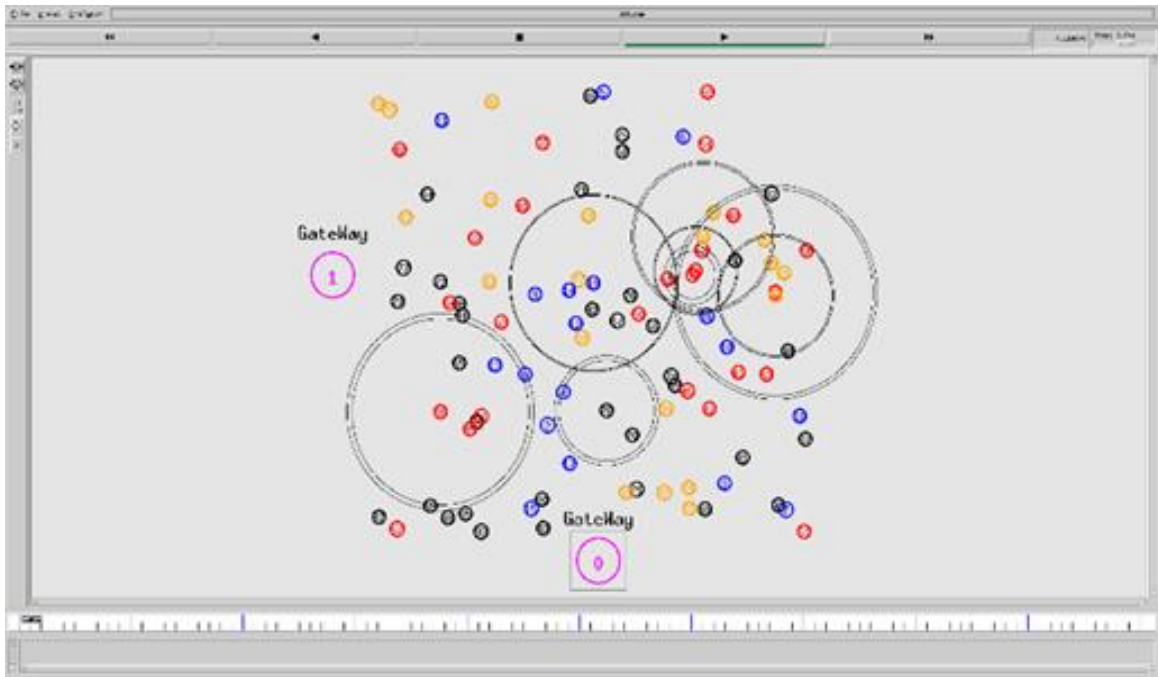


Figure 2. Structure of cluster submission

The parameters to calculate weight value was assumed here that as follows:

Mobility of nodes (10km/hr to 30 km/hr)

Distance between nodes (0.1km to 0.9km)

Battery power consumed using the formula to calculate the weight (20 Ampere-hour to 70 Ampere-hour)

Table 2. Cluster no. 1 of nodes

Node ID	Weigh Value
1	$W1 = 0.7 * 6 + 0.2 * 1.2 + 0.06 * 10 + 0.04 * 30 = 6.24$
2	$W2 = 0.7 * 4 + 0.2 * 0.35 + 0.06 * 20 + 0.04 * 70 = 6.87$
3	$W3 = 0.7 * 4 + 0.2 * 0.4 + 0.06 * 25 + 0.04 * 60 = 6.78$
4	$W4 = 0.7 * 3 + 0.2 * 0.1 + 0.06 * 23.6 + 0.04 * 50 = 6.24$
5	$W5 = 0.7 * 5 + 0.2 * 0.35 + 0.06 * 15 + 0.04 * 70 = 7.27$
6	$W6 = 0.7 * 3 + 0.2 * 0.5 + 0.06 * 20 + 0.04 * 70 = 6.50$
7	$W7 = 0.7 * 4 + 0.2 * 0.45 + 0.06 * 26 + 0.04 * 60 = 6.85$

Table 3. Cluster no. 2 of nodes

Node ID	Weight Value
14	$W_{14} = 0.7 * 4 + 0.2 * 0.6 + 0.06 * 15 + 0.04 * 30 = 5.02$
6	$W_6 = 0.7 * 3 + 0.2 * 0.5 + 0.06 * 20 + 0.04 * 70 = 6.50$
17	$W_{17} = 0.7 * 3 + 0.2 * 0.9 + 0.06 * 25 + 0.04 * 50 = 7.4$
18	$W_{18} = 0.7 * 4 + 0.2 * 0.57 + 0.06 * 20 + 0.04 * 40 = 5.74$
19	$W_{19} = 0.7 * 3 + 0.2 * 0.5 + 0.06 * 18 + 0.04 * 60 = 5.02$

Table 4. Cluster no. 3 of nodes

Node ID	Weight Value
9	$W_9 = 0.7 * 4 + 0.2 * 0.8 + 0.06 * 10 + 0.04 * 20 = 4.36$
3	$W_3 = 0.7 * 4 + 0.2 * 0.4 + 0.06 * 25 + 0.04 * 60 = 6.78$
10	$W_{10} = 0.7 * 3 + 0.2 * 0.9 + 0.06 * 25 + 0.04 * 60 = 6.18$
13	$W_{13} = 0.7 * 2 + 0.2 * 0.7 + 0.06 * 30 + 0.04 * 65 = 5.94$
15	$W_{15} = 0.7 * 3 + 0.2 * 0.8 + 0.06 * 26 + 0.04 * 60 = 6.22$

5. CONCLUSION

For security of networks in MANET, secure key transfer is important. It is difficult to know the dependable nodes in MANET network without the idealistic concept of the intermediate node identity in operation. Ad hoc network is a type of networks that do not rely on any infrastructure during establishment. Where intruders can monitor and intercept the password, authentication key transfer in MANET networks via nameless midway nodes is not suitable to be used. It is imperative to use a strong secure method of key transfer that hides data of verification keys. Thus, this proposed system is suitable where key is hidden in the image from the system that is different from others in order to secure key transfer in MANET networks. The image then splits into two parts while the parts are therefore encrypted for double level of security. Ability to develop a doubled level of security of key transfer in the networks of MANET with encrypted secure key transfer is the primary advantage of the future approach. A cluster head is responsible for routing process in cluster-based routing protocol and information like cluster links and membership are maintained by this cluster head in accordance to which what it is possible to dynamically discover the inter-cluster routes. Thus, A forecasted weighted clustering algorithm is proposed in this study where more eligible and proper nodes are selected as cluster head as well as introducing server node to reduce per node calculation overhead.

Abbreviations and Acronyms

ID	Abbreviations	
1	MANET	Mobile ad hoc network
2	FWCA	Forecast Weighted Clustering Algorithm
3	WCA	Weighted Clustering Algorithm
4	DIP	Digital Image Processing
5	UDP	User Datagram Protocol
6	EMA	Exponential Moving Average
7	FW	Forecasted Weight

REFERENCES

- [1] R. C. Gonzalez and R. E. Woods, "Digital Image Processing," Pearson Prentice Hall, 2008.
- [2] R. Chadha and A. Aushik, "Original Approach With Image Processing For Securing Ad-Hoc Network," *International Journal of Core Engineering & Management (IJCEM)*, vol. 1, no. 8, pp. 10-15, Nov 2014.
- [3] M. H. Abdulameer, et al., "Face recognition technique based on adaptive-opposition particle swarm optimization (AOPSO) and support vector machine (SVM)," *ARNP Journal of Engineering and Applied Sciences*, vol. 13, pp. 2259-2266, Mar 2018.
- [4] J. Amudha, N. Pradeepa, and R. Sudhakar, "A survey on digital image restoration," *Elsevier Procedia Engineering*, vol. 38, pp. 2378-2382, 2012.
- [5] H. Moudni, et al., "Secure routing protocols for mobile ad hoc networks," *2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez*, pp. 1-7, 2016.
- [6] A. E. C. Pandelea, et al., "Image processing using artificial neural networks," *Bulletin of the Polytechnic Institute of Jassy – Constructions, Architecture Section*, vol. 61, no. 65, pp. 9-21, 2015.
- [7] J. Kundu, et al., "An Efficient Trust-Based Routing Scheme by Max-Min Composition of Fuzzy Logic for MANET," *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*, 2016, pp. 435-440.

- [8] Suresha D. and Prakash H. N., "A Novel Approach Using Image Processing for Securing Ad-Hoc Networks," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 2, pp. 9295-9301, Feb 2014.
- [9] I. A. Alameri and G. Radchenko, "Development of Student Information Management System based on Cloud Computing Platform," *Journal of Applied Computer Science & Mathematics*, vol. 11, no. 2, pp. 9-14, 2017.
- [10] I. A. Alameri and G. Radchenko, "Cloud computing and websites design and development," Lambert academic publishing, Jul 2016.
- [11] I. A. Alameri, "A Novel approach to comparative analysis of legacy and nature inspired ant colony optimization based routing protocol in MANET," *Journal of Southwest Jiaotong University*, vol. 54, no. 4, 2019.
- [12] M. B. M. Kamel, et al., "STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET," *Proceedings of 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2017*, Mar 2017, pp. 1278-1282.
- [13] Sathisha M. S., et al., "Implementation of Protected Routing to Defend Byzantine Attacks for MANET's," *International Journal of Advanced Research in Computer Science*, vol. 3, no. 4, pp. 109-114, 2012.
- [14] A. Tønnesen, "Mobile Ad-Hoc Networks," <http://www.olsr.org/docs/wos3-olsr.pdf>.
- [15] P. Dipesh and N. Rakesh, "Ad hoc Wireless Networks," <http://www.acsu.buffalo.edu/~nagi/courses/684/adhoc.pdf>.
- [16] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE network, special issue on network security*, 1999. <http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf>.
- [17] H. Luo, et al., "Self-securing Ad Hoc Wireless Networks," *Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02)-IEEE*, Jul 2002.
- [18] Piyalikar, et al., "Forecast Weighted Clustering in MANET," *Procedia - Procedia Computer Science, Twelfth International Multi-Conference on Information Processing (IMCIP-2016)*, vol. 89, pp. 253-260, 2016.
- [19] D. Ravilla and C. S. R. Putta, "Enhancing the Security of MANETs Using Hash Algorithms," *Procedia - Procedia Computer Science, Eleventh International Multi-Conference on Information Processing (IMCIP-2015)*, vol. 54, pp. 196-206, 2015.
- [20] FIPS PUB 180-4, "Secure Hash Standard (SHS)," Information Technology Laboratory, National Institute of standards and Technology Gaithersburg, MD 20899-8900, Mar 2012.
- [21] S. M. S. S. D., "Implementation of Secure Biometric Authentication Using Kerberos Protocol," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 249-254, 2013.
- [22] S. Wiedenbeck, et al., "Authentication Using Graphical Passwords: Basic Results," *Proceeding: SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security*, pp. 1-12, Jul 2005.
- [23] R. B. Wolfgang and E. J. Delp, "Overview of image security techniques with applications in multimedia systems," *Proc. SPIE 3228, Multimedia Networks: Security, Displays, Terminals, and Gateways*, Feb 1998.
- [24] H. N. Saad and M. B. M. Kamel, "Weight analysis for weighted cluster algorithms in mobile ad-hoc network weight analysis for weighted cluster algorithms in mobile ad-hoc network," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 14, pp. 3352-3364, Jul 2017.
- [25] S. Dhamodharavadhani, "A survey on clustering based routing protocols in Mobile ad hoc networks," *International Conference on Soft-Computing and Networks Security (ICSNS)*, Coimbatore, pp. 1-6, 2015.
- [26] N. Agarwala, "Mobile Ad hoc Networks and its Clustering Scheme," *International Journal of Science and Research*, vol. 1, no. 3, pp. 36-43, Dec 2012.
- [27] P. Kar, M. K. D. Barma, S. Roy and S. K. Sen, "Energy Efficient Weight Based Clustering in MANET," *2nd International Conference on Data Engineering and Communication System (ICDECS)*, vol. 10, pp. 82-86, Dec 2015.
- [28] Y. Sato, A. Koyama, and L. Barolli, "A Zone Based Routing Protocol for Ad Hoc Networks and Its Performance Improvement by Reduction of Control Packets," *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*, IEEE Computer Society, Fukuoka, pp. 17-24, 2010.
- [29] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Huang SH., MacCallum D., Du DZ. (eds) *Network Security*. Springer, Boston, MA, pp. 117-142, 2010.
- [30] P. Kar, M. Kanti, and D. Barma, "Forecast Weighted Clustering in MANET," *Twelfth International Multi-Conference on Information Processing (IMCIP-2016)*, vol. 89, pp. 253-260, 2016.

BIOGRAPHIES OF AUTHORS



Ibrahim Alameri is currently a PhD student at Pardubice university-Czech Republic. Additionally, he is working as an assistant lecturer in College of Medicine-Jabir Ibn Hayyan Medical University. He earned a Master degree in computer science from South Ural State University. Mr. Alameri has eight years of research experience. His research fields are Mobile ad hoc networks, protocol optimizations and cloud computing.



Jawad Kadhim Mutar is an assistant lecturer in history department in the educational college of Humanities in almuthana university. He earned his master in computer science in osmaniah university.



Ameer N. Onaizah is an assistant lecturer in College of Computer Science and Mathematics university of Kufa. Currently, he is a PhD student at Beijing Institute of Technology, China



Iftikhar Ahmed Koondhar is currently PhD student at Beijing Institute of Technology, China. He is working as an assistant professor in the department of computer systems engineering in Quaid-e-awam University-Pakistan. Mr. Koondhar earned his Master of Engineering degree in Communication Systems and Networks from Mehran University of Engineering and Technology - Pakistan. His research interests include computer networks, data mining and high-performance computing and internet of things.