Enhancing the security of quality of service-oriented distributed routing protocol for hybrid wireless network

Miaad Husam Mahdi, Ibrahim Adel Ibrahim
Department of Computer Engineering, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Jul 15, 2022
Revised Sep 19, 2022
Accepted Sep 29, 2022

Keywords:

Cryptography
Hybrid wireless networks
Message authentication code
Network simulator NS2
Routing protocols

ABSTRACT

Merging the wireless infrastructure network with the wireless mobile ad-hoc networks constitutes hybrid wireless networks (HWNs). Quality of service (QoS) demands are available with the help of HWNs. However, these networks are subjected to many types of attacks because of their open wireless medium. To enhance the security of HWNs, it is necessary to provide secure routing protocols. Several routing protocols have been proposed for HWNs, one of them is the quality of service-oriented distributed (QOD) routing protocol. In this paper, two security mechanisms have been proposed for the QOD protocol. The first mechanism is used to protect transmitted data in the network using asymmetric and symmetric cryptography. The second mechanism has been proposed to enhance the security of the QOD routing protocol using keyed hash message authentication code (HMAC). The second security mechanism assumed that there is a secret key shared between each pair of neighbor nodes. Also, asymmetric cryptography is used to exchange the secret key. The secret key is used to include the message authentication code (MAC) for each message exchanged between the neighbor nodes. A network simulator NS2 is used to simulate our proposed schemes.

Corresponding Author:

Miaad Husam Mahdi
Department of Computer Engineering, University of Technology
Baghdad, Iraq
Email: ce.20.06@grad.uotechnology.edu.iq

1. INTRODUCTION

The evolution of wireless networks has led to many wireless applications that are used in different fields, including education, commerce, emergency services, entertainment, military, and health. Wireless networks are much better than wired networks in terms of costs and have also improved in technology in the past few decades. Currently, people want to hold conferences via mobile devices wirelessly during navigation, playing games, and watching videos. Real-time multimedia applications need to support quality of service (QoS) as they reduce transmission time and improve throughput in wireless networking environments to ensure easy communication between wireless infrastructures and mobile devices [1]–[3].

Hybrid networks are the networks resulting from the integration of infrastructure with mobile ad-hoc networks (MANET) networks to benefit from each other (specifically scalability) and have proven to be the best network architecture for the next generation. Hybrid networks can help to process QoS requirements for many different applications [4], [5]. Many QoS requirements for different applications can be addressed with hybrid wireless networks (HWNs) that have been confirmed to be a better network structure for wireless networks. A hybrid wireless network merges MANETs and infrastructure wireless networks to power their advantage and ride their shortcomings, and finally enhance the wireless network performance. Specifically, the

MANET's scalability is improved by HWNs while the infrastructure network coverage is extended by MANETs [6], [7].

MANETs are collections of mobile nodes that contain wireless transmitters and receivers. These nodes communicate with each other in a multi-hop manner via wireless links. One of the main advantages of wireless networks is their capability to permit data transmission among different parties with maintaining their mobility. However, this transmission is bounded by the range of transmitters [8], [9]. This means that no communication can be done beyond the transmission range of the communicating nodes. MANET solves this difficulty by letting intermediate nodes relay data to other nodes [10], [11] to achieve this, two types of MANET are applied, multihop and single hop. In a multihop networks, nodes depend on their neighbor nodes to transmit to their destination in case of this destination location is out of the range of the source node. On the other hand, direct transmission is applied among nodes in a single hop network. MANET is able of making a self-maintaining and self-configuring network without a centralized infrastructure, which is often impracticable in climacteric mission applications such as military combat or disaster recovery [12].

2. BACKGROUND AND RELATED WORK

The routing protocols are critical components that affect the performance of wireless networks in data communication. Also, securing routing protocols are necessary to maintain the security of the wireless networks. So, many researccchers worked on enhancing the security of the routing protocols in different applications [13]. Hu *et al.* [14] attempt to authenticate the routing updates of the destination-sequenced distance-vector (DSDV) [15] routing protocol to keep safe the sequence number and the metric. However, this protocol is vulnerable to some attacks by malicious nodes such as increasing the route metric more than once and including the previous metric and hash value received on its own. These two problems are addressed in the super SEAD routing protocol [16], [17].

Wan *et al.* [18] enhance the security of the DSDV routing protocol so that attacker nodes can't increase or decrease the distances metrics as long as no two nodes are conspiring. The assumption made by this protocol is that every node in the network shares a secret key with the other nodes in this network. Kumar and Mohideen [19] proposes (SARP-HWNs) routing protocols to minimize link failure in the present routing path and can provide quick recovery, enhance throughput, decrease end-to-end latency, optimize the lifetime of the routing path without compromising energy consumption, and QoS when compared to other existing strategies. Guo *et al.* [20], proposed (HODVM) routing protocol for (HWNs). This protocol includes separating the network to backbone network and non-backbone [21]-[23] to carry out the static and dynamic routing, respectively. Shen *et al.* [9], Li *et al.*, [24] in presented A distributed three-hop routing protocol (DTR) for networks that used hybrid wireless networks. DTR cuts up the stream of the message by the source into segments and then sends these segments concurrently to different base stations. DTR routing protocol makes full use of base stations and increases the throughput of the network. Moreover, this protocol reduced overhead by removing route discovery and maintenance. Also, the DTR protocol avoided overloading base stations because it has a congestion control algorithm [24].

Another routing protocol proposed [7], [25] for HWNs. This protocol provides quality of service services for different applications that need a low delay, reduced transmission time, and increased throughput through using five algorithms which are discussed in the next subsections. However, some mentioned routing protocols didn't address the security issues in HWNs. Any malicious node advertises fake data which can't be checked out due to the absence of security in these routing protocols [26], [27]. The quality of service-oriented distributed (QOD) is one of the protocols that have no security mechanisms according to our knowledge. So, to enhance the security of the QOD protocol, two security mechanisms have been proposed for this protocol.

The rest of the paper is categorized as following: section 3.1 presents specifications and elaborates on all the algorithms of the QOD routing protocol. Section 3.2 elaborates on the problem definition. The proposed work are presented in section 3.3. Section 4 presents the obtained results and provides a comparison with QOD routing protocol. Finally, section 5 outlines the conclusion of this paper.

3. QOS-ORIENTED DISTRIBUTED ROUTING PROTOCOL

The QOD routing protocol is proposed for the hybrid wireless network. The hybrid wireless network consists of base stations and mobile nodes as shown in Figure 1. For example, when source node n1 wants to transmit a data packet it can choose one of two ways. The first way, the node n1 can transmit its data directly to the access point (AP) when this AP satisfies QoS requirements. Or, it can request its neighbors to assist in the transmission of its data [7], [25].

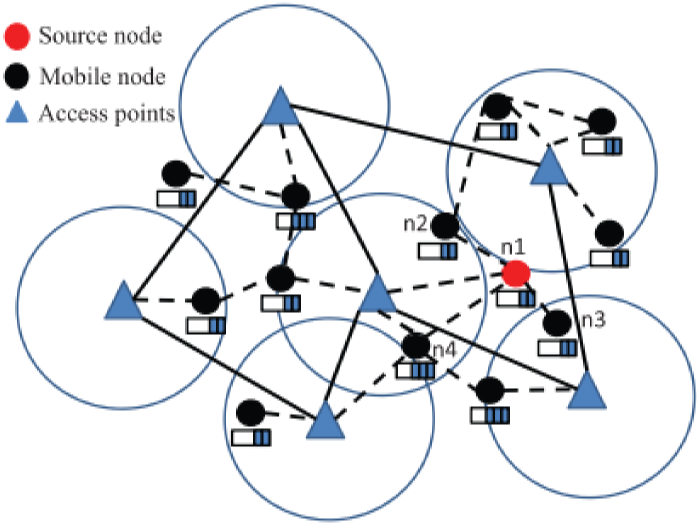


Figure 1. Hybrid wireless network [8]

3.1. Scheme description

When the link between an AP and the source node didn't satisfy the QoS, the source node sends a request message to its neighbors to assist it in the transmission of its data. On receiving the forward message by neighbor nodes. It sends reply messages containing the resources available. The replied neighbors that guarantee the QoS requirements are selected by the source node. Those selected neighbors periodically send their statuses to the source node. The source node schedules its packets to the selected qualified neighbor nodes using round robin fashion [7], [25]. Five algorithms used by the QOD routing protocol include the following:

a) Earliest deadline first scheduling algorithm (EDF): intermediate nodes used this algorithm to forward packets. This algorithm assigns the highest priority to the packet with the nearest deadline. And it sends the packet with the highest priority first.

b) Distributed packet scheduling algorithm: this algorithm is proposed to further reduce the total transmission time of the overall packet stream. This algorithm sends packets that are generated first to relay nodes with higher queueing delays and packets that are generated next to relay nodes with lower queueing delays.

c) Mobility-based segment resizing algorithm: when the packet size is reduced, the intermediate node scheduling feasibility is increased and the probability of packet dropping is reduced. The basic idea of this algorithm is that larger size packets are transmitted to intermediate nodes with lower mobility. Whereas smaller-size packets are sent to intermediate nodes with higher mobility.

d) Least slack first (LSF) scheduling algorithm: EDF algorithm is suitable for some applications that tend to be hard-deadline driven. But, it did not provide fairness for the applications that tend to be soft-deadline driven. So, the LSF algorithm is used to achieve fairness in packet forwarding.

e) Data redundancy elimination-based transmission: packets can be overheard and cached by APs and mobile nodes because of the broadcasting feature for the wireless networks, the APs and mobile nodes can overhear and cache packets. So, this algorithm eliminates redundant data by reducing the message sizes. Thus, exploiting the above feature of wireless networks to increase the scheduling feasibility and enhance the QoS overall performance of the routing.

3.2. Problem definition

The QOD routing protocol assumes reliable participants; that is, all nodes are trusted. However, as hybrid wireless networks consisted of wireless links, they are susceptible to many attacks including message distortion, message reply, passive eavesdropping, and active impersonation. These attacks come from inside or outside the network. For example, the scheduling algorithm of the QOD routing protocol may be disrupted if a malicious node arbitrarily tampered with the update messages. Thus, securing the QOD routing protocol is necessary to define against malicious attacks exchange the secrete key between any two pairs of neighbor nodes.

3.3. Proposed work

Two mechanisms are proposed in this paper to protect data in hybrid wireless networks. The first mechanism used RSA and AES algorithms. However, symmetric cryptography suffers from key distribution problems. Therefore; the RSA algorithm is used to deal with key distribution. Since encryption using symmetric-key algorithms is faster than public-key algorithms, the AES algorithm was used to encrypt the transmitted data. The second mechanism is proposed to enhance the security of the QOD routing protocol using the keyed-hash message authentication code (HMAC). The latter mechanism assumes that each pair of neighbor nodes have a shared secret key as shown in Figure 2. The source node sends a request message for the public key of its neighbor node. Then, it encrypts the shared secret key using this received public key and sends it to its neighbor. Algorithm 1 shows the pseudo-code for the enhanced QOD routing protocol.

Algorithm 1. Developed pseudo-code for the QOD routing

```
If receive a packet forwarding request from a source node then
    If validation of message authentication code is ok then
        If this.SpaceUtility<threshold then
            Reply to the source node and append message authentication code.
        End if
    End if
End if
If receive forwarding request replies for neighbor nodes then
    If validation of message authentication code is ok then
        Determine the packet size to each neighbor.
        Estimate the queuing delay for the packet for each neighbor.
        Determine the qualified neighbors that can satisfy the deadline requirements.
        Sort the qualified nodes in descending order.
        Allocate workload rate for each node.
        For each intermediate node $n_i$ in the sorted list do
            Send encrypted packets to $n_i$.
        End for
    End if
End if
```

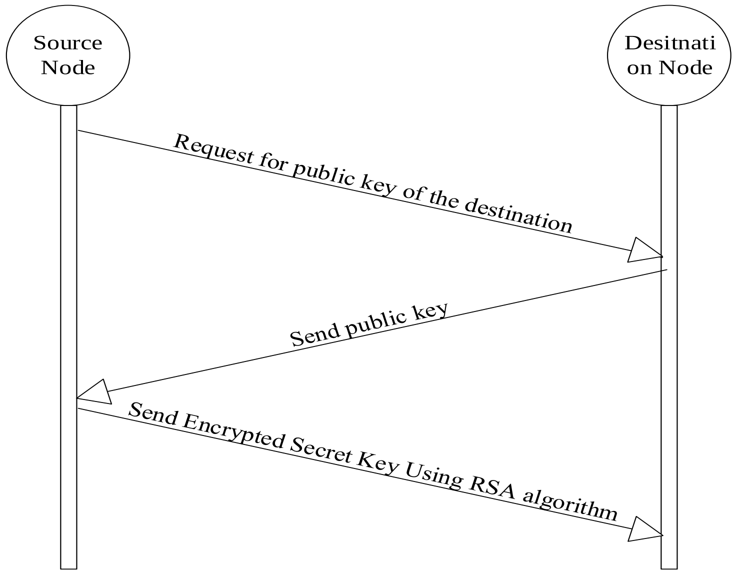

Source Node
Desitnati on Node
Request for public key of the destination
Send public key
Send Encrypted Secret Key Using RSA algorithm

Figure 2. Secret key sharing between the source and the destination

Also, to authenticate the neighbor node, the sender appends a message authentication tag with each routing update for each neighbor. To authenticate a routing update message using the secret key K the legitimate source node used a secure hash algorithm (SHA-2) with HMAC as a cryptographic hash function. The source node S will transmit the routing update message with the resulting message authentication code (MAC) to its neighbor node. The neighbor node R, on receipt of the routing update message and the tag value, will generate the MAC value for the received message using the pre-shared secret key. Then it will compare this generated MAC with the received MAC. If the two MACs are matched then the node is authentic and the integrity of the received routing update message is valid. Otherwise, the message authentication codes are not matched and the received routing update message is dropped [28]. This scenario is shown in Figure 3.

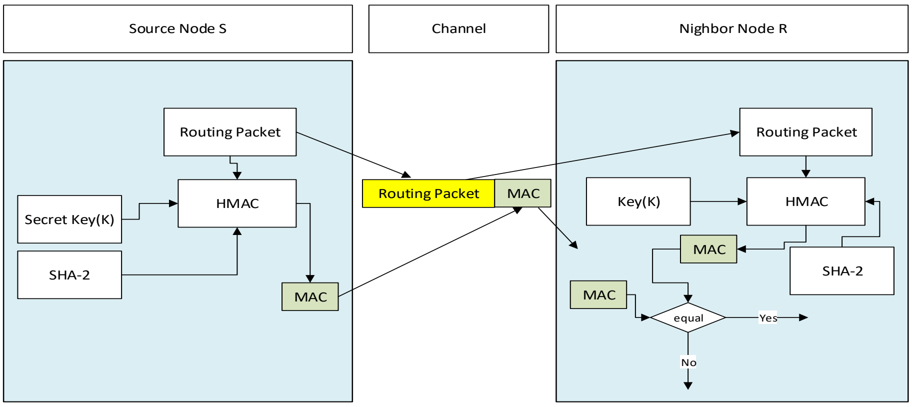


Figure 3. Key hash message authentication code mechanism

4. SIMULATION AND RESULTS

In the simulation, nine access points with IEEE 802.11 MAC protocol are distributed in the area. Two source nodes are selected arbitrarily to send packets to AP every 10 seconds. The constant bit rate (CBR) is used to generate the nodes' traffics at the rate of 100 kb/s. Nodes speeds are randomly selected from [1–50] m/s. other parameters concerning the hybrid wireless network are explained in the following Table 1.

Table 1. The parameters of the wireless hybrid network

Simulation parameters	Value
Environment size	1,000 m×800 m
Application	CBR
Transport protocol	UDP
Nodes	Different number of nodes
APs	Different number
Transmission range	250 m
Simulation time	200 s
Network	Wireless

4.1. Performance evaluation

A comparison is done between the QOD [25] and the proposed work in terms of throughput by changing the number of nodes, changing their speed, and increasing workloads. AWK scripts were used to handle the trace files obtained by the simulations. The figures below were created using the average values of packet delivery ratio (PDR), normalized routing load, throughput, and E2E when the number of nodes, interconnections, velocity, and time were changed.

4.1.1. Performance with different mobility speeds

Node's mobility speed was arbitrarily selected from (1-40) m/s. Figure 4 shows the QoS throughputs of the QOD routing protocol [7], [25] and the proposed work versus the node mobility speed. The throughputs of the two schemes decrease when node mobility increases. This is because higher mobility causes link failures that lead to packet drops. The proposed work's throughput competes with the QOD's throughput. However, security mechanisms can predominantly disturb network performance.

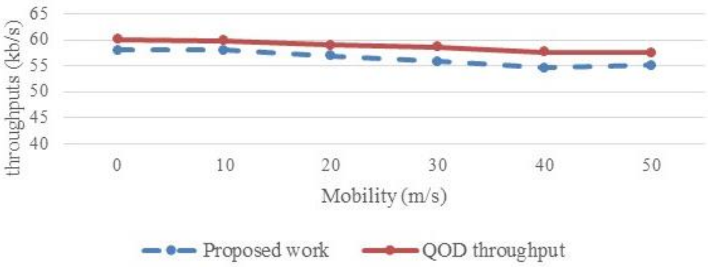


Figure 4. Throughput versus mobility

The overhead rate is the size of all control packets generated at one second. Figure 5 shows the overhead rates of the QOD [7], [25], and proposed work. The overhead of the two schemes is increased when the node mobility increases. Also, the overhead of the proposed work is more than the overhead of the QOD because of the HMAC authentication mechanism used to enhance the security of the QOD routing protocol [7], [25].

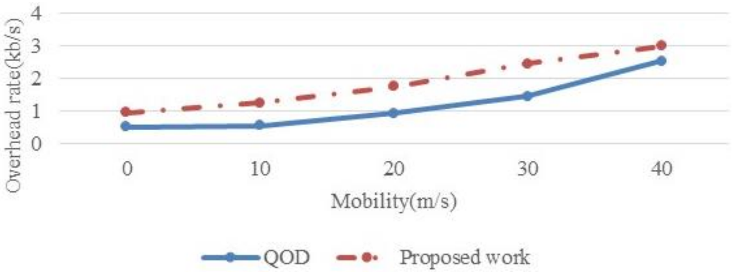


Figure 5. Overhead versus mobility

4.1.2. Performance with different number of APs

Figure 6 explains the QoS throughput versus the number of base stations. Higher throughput is produced when the number of access points is increased for the two schemes. This is because path lengths are reduced by increasing the number of access points. Since no security mechanisms are employed in the QOD protocol, its throughput is more than our proposed work throughput. As explained earlier, the security mechanisms often hinder the performance of the network. So, there is a tradeoff between network performance and security.

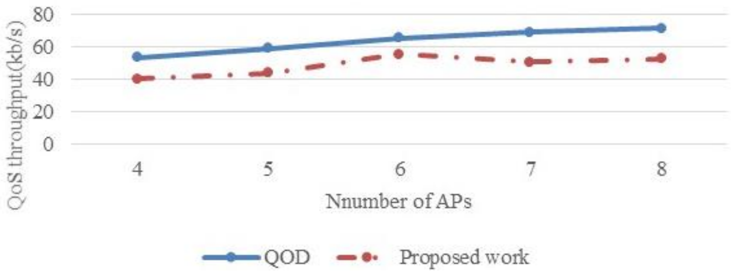
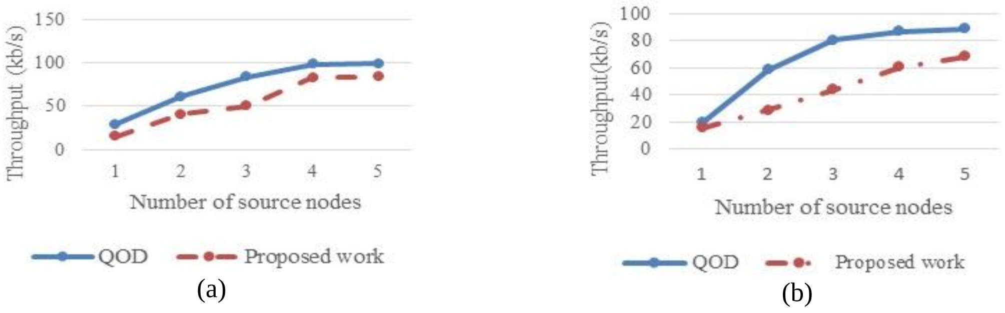


Figure 6. Throughput versus APs

4.1.3. Performance with different workloads

Figure 7 shows the throughput against the number of source nodes with differnet moblity. Figures 7 (a) and (b) show the throughput of the two schemes versus the number of source nodes with average node mobilities 0 m/s and 20 m/s, respectively. Though, nodes' motilities are chosen randomly from the range 0 m/s to 20 m/s. when the number of source nodes is increased, the workload of the two schemes is also increased. The throughput is increased linearly as the number of source nodes increased from 1 to 3. The throughput of our proposed work competes with QOD throughputs.



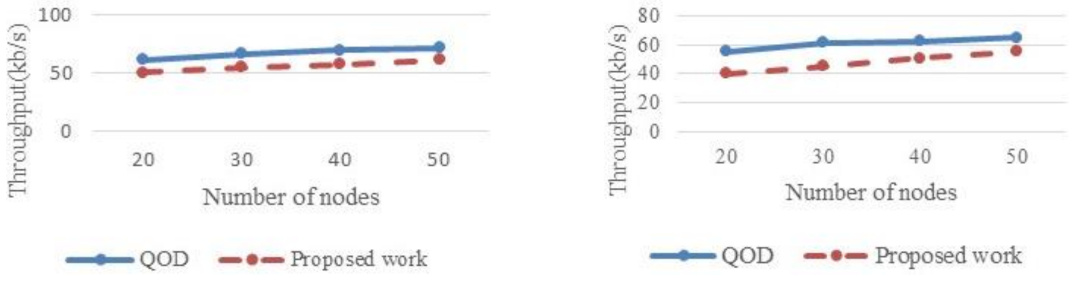
(a)

(b)

Figure 7. Throughput against the number of source nodes at (a) mobility=0 m/s and (b) mobility=20 m/s

4.1.4. Performance with different network sizes

Figure 8 shows the throughput of the two routing protocols with different network sizes. So, Figure 8 (a) and (b) show the QoS throughput of the two schemes with different networks size in terms of the number of nodes against the mobility speed of 0 m/s and 20 m/s, respectively. Both figures illustrate that the throughput increases with increasing the number of nodes for both the QOD and the proposed work.



(a) (b)

Figure 8. Throughput with different network sizes at (a) mobility=0 m/s and (b) mobility=20 m/s

5. CONCLUSION

In this paper, we have improved the security of the QOD protocol. This included data encryption using the AES algorithm to provide confidentiality for the transmitted messages and also the use of the RSA algorithm for symmetric key exchange. Also, an HMAC mechanism is used to ensure the integrity and authenticity of the routing table information to verify that the nodes that send data to the rest of the network are not malicious. A network simulator NS2 is used to verify our proposed work. The obtained results in terms of throughput by changing the number of nodes, changing their speed, and increasing workloads are compared with the QOD protocol. The obtained throughputs compete with the QOD protocol. The proposed work can be improved further in terms of performance and security. Also, other experiments will be done to further analyze the behavior of the proposed work.

REFERENCES

[1] J. I. Naser and A. J. Kadhim, “Multicast routing strategy for SDN-cluster based MANET,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 5, pp. 4447–4457, 2020, doi: 10.11591/ijece.v10i5.pp4447-4457.

[2] W. Dai, I. Ibrahim, and M. Bassiouni, “An Improved Replica Placement Policy for Hadoop Distributed File System Running on Cloud Platforms,” in *Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017*, pp. 270–275, 2017, doi: 10.1109/CSCloud.2017.65.

[3] W. Dai, I. Ibrahim, and M. Bassiouni, “Improving Load Balance for Data-Intensive Computing on Cloud Platforms,” *Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016*, pp. 140–145, 2016, doi: 10.1109/SmartCloud.2016.44.

[4] I. A. Ibrahim, W. Dai, and M. Bassiouni, “Intelligent Data Placement Mechanism for Replicas Distribution in Cloud Storage Systems,” in *Proceedings - 2016 IEEE International Conference on Smart Cloud, SmartCloud 2016*, 2016, pp. 134–139, doi: 10.1109/SmartCloud.2016.23.

[5] I. A. Ibrahim and M. Bassiouni, “Improving MapReduce Performance with Progress and Feedback Based Speculative Execution,” in *Proceedings - 2nd IEEE International Conference on Smart Cloud, SmartCloud 2017*, 2017, pp. 120–125, doi: 10.1109/SmartCloud.2017.25.

[6] S. Aakasham and S. R. Mugunthan, “A secure QoS oriented distributed routing protocol for hybrid wireless networks,” *Int. J. Appl. Eng. Res.*, vol. 10, no. 20, pp. 18169–18175, 2015, doi: 10.17148/ijarcce.2015.4112.

[7] Z. Li and H. Shen, “A QoS-oriented distributed routing protocol for hybrid wireless networks,” *IEEE Trans. Mob. Comput.*, vol. 13, no. 3, pp. 693–708, 2014, doi: 10.1109/TMC.2012.258.

[8] L. Shen, Haiying and Li, Ze and Yu, “A Distributed Three-Hop Routing Protocol to Increase the Capacity of Hybrid Wireless Networks,” *IEEE Trans. Mob. Comput.*, vol. 14, no. 10, pp. 1975–1991, 2015, doi: 10.1109/TMC.2015.2388476.

[9] I. A. Ibrahim and M. Bassiouni, “Improvement of data throughput in data-intensive cloud computing applications,” *Proc. - 5th IEEE Int. Conf. Big Data Serv. Appl. BigDataService 2019, Work. Big Data Water Resour. Environ. Hydraul. Eng. Work. Medical, Heal. Using Big Data Technol.*, pp. 49–54, 2019, doi: 10.1109/BigDataService.2019.00013.

[10] W. Dai, I. Ibrahim, and M. Bassiouni, “An Improved Straggler Identification Scheme for Data-Intensive Computing on Cloud Platforms,” in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 211--216, doi: 10.1109/CSCloud.2017.64.

[11] I. A. Ibrahim and M. Bassiouni, “Improvement of job completion time in data-intensive cloud computing applications,” *J. Cloud Comput.*, vol. 9, no. 1, 2020, doi: 10.1186/s13677-019-0139-6.

[12] B. Ul Islam Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, “A survey on MANETs: Architecture, evolution, applications, security issues and solutions,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 832–842, 2018, doi: 10.11591/ijeecs.v12.i2.pp832-842.

[13] R. B. Al-Bayram and R. M. Abdullah, “Network size variation of geographical aided routing protocols in MANET,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 420–428, 2021, doi: 10.11591/ijeecs.v21.i1.pp420-428.

[14] Y. C. Hu, D. B. Johnson, and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, 2003, doi: 10.1016/S1570-8705(03)00019-2.

[15] C. E. Perkins, P. Bhagwat, C. E. Perkins, P. Bhagwat, C. E. Perkins, and P. Bhagwat, “Highly Dynamic (DSDV) for Mobile Computers Routing,” *Proc. ACM SIGCOMM94, London, UK*, vol. 24, no. 4, pp. 234–244, 1994, [Online]. Available: http://portal.acm.org/citation.cfm?doid=190809.190336.

[16] M. Boulaiche, *Survey of Secure Routing Protocols for Wireless Ad Hoc Networks*, vol. 114, no. 1. Springer US, 2020.

[17] B. Soediono, *Security for Wireless AD Hoc Networks*, vol. 53. 1989.

[18] T. Wan, E. Kranakis, and P. C. Van Oorschot, “Securing the destination-sequenced distance vector routing protocol (S-DSDV),” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3269, pp. 358–374, 2004, doi: 10.1007/978-3-540-30191-2_28.

[19] A. V. Kumar and S. K. Mohideen, “Security aware routing protocol for hybrid wireless network (SARP-HWNs) via trust enhanced mechanism,” *Int. J. Bus. Data Commun. Netw.*, vol. 15, no. 1, pp. 34–57, 2019, doi: 10.4018/IJBDCN.2019010103.

[20] L. Guo *et al.*, “Design on routing protocol in hybrid wireless self-organizing networks,” *Proc. - 2010 2nd IEEE Int. Conf. Netw. Infrastruct. Digit. Content, IC-NIDC 2010*, pp. 569–573, 2010, doi: 10.1109/ICNIDC.2010.5657832.

[21] M. A. Jubair *et al.*, “Competitive analysis of single and multi-path routing protocols in MANET,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 1, pp. 293–300, 2020, doi: 10.11591/ijeecs.v19.i1.pp293-300.

[22] W. Dai, I. Ibrahim, and M. Bassiouni, “A New Replica Placement Policy for Hadoop Distributed File System,” *Proc. - 2nd IEEE Int. Conf. Big Data Secur. Cloud, IEEE BigDataSecurity 2016, 2nd IEEE Int. Conf. High Perform. Smart Comput. IEEE HPSC 2016 IEEE Int. Conf. Intell. Data S*, no. April 2016, pp. 262–267, 2016, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.30.

[23] Z. L. and H. Shen, “A Distributed Three-Hop Routing Protocol to Increase the Capacity of Hybrid Wireless Networks,” in *2009 International Conference on Parallel Processing*, 2009, vol. 14, no. 10, pp. 277--284, doi: 10.1109/TMC.2015.2388476.

[24] M. H. Mahdi and I. A. Ibrahim, “Routing protocols for hybrid wireless networks : a brief review,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 2, pp. 1–7, 2022, doi: 10.11591/ijeecs.v27.i2.pp1-1x.

[25] Z. Li and H. Shen, “A QoS-oriented distributed routing protocol for hybrid wireless networks,” *IEEE Trans. Mob. Comput.*, vol. 13, no. 3, pp. 693–708, 2014, doi: 10.1109/TMC.2012.258.

[26] M. Mohanapriya, N. Joshi, and M. Soni, “Secure dynamic source routing protocol for defending black hole attacks in mobile Ad hoc networks,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 1, pp. 582–590, 2021, doi: 10.11591/ijeecs.v21.i1.pp582-590.

[27] U. Kumaran, A. Ramachandran, J. Jegan, and E. K. Subramanian, “Enhanced routing for secured ad-hoc network,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 19, no. 2, pp. 949–956, 2020, doi: 10.11591/ijeecs.v19.i2.pp949-956.

[28] Y. N. Hatif, Y. A. Abbas, and M. H. Ali, “Lightweight ANU-II block cipher on field programmable gate array,” *Int. J. Electr. Comput. Eng.*, vol. 12, no. 3, pp. 2194–2205, 2022, doi: 10.11591/ijece.v12i3.pp2194-2205.

BIOGRAPHIES OF AUTHORS

Miaad Husam Mahdi received the B.Sc. (1st Class Hons.) Degree in Computer Engineering from University of Diyala, Iraq, in 2015. He is a staff member in Diyala University, Iraq. He is currently a M.Sc. student at the University of Technology, Computer Engineering Department, Iraq. His research interests are in computer engineering, computer networks, cryptography, FPGA, wireless ad-hoc networks and image processing. She can be contacted at email: ce.20.06@grad.uotechnology.edu.iq.

Ibrahim Adel Ibrahim received the B.Sc. degree in Computer Engineering Department from college of Engineering, Mustansiriyah University, Iraq, the M.Sc. degree in Computer Engineering, University of Technology, Iraq, and the Ph.D. degree in Computer Engineering, Florida, USA, 2019. He has supervised and co-supervised masters’ students. He has authored or coauthored more than 9 publications with 6 H-index and more than 110 citations. His research interests include Cloud Computing networks, Mobile cloud computing, BigData, and computer networks. He can be contacted at email: Ibrahim.a.almotairi@uotechnology.edu.iq.