International Journal of Engineering & Technology, 12 (2) (2023) 31-37

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Improve the quality of service through secure routing networks secured in the mail

Aseil Nadhum Kadhum *

University of Babylon
**Corresponding author E-mail: easeel18@yahoo.com*

Abstract

A mobile ad hoc network (MANET) is a stand-alone system with mobile nodes. Nodes can move around at will. Communication is subject to security breaches without a centralized, secure infrastructure, and the nodes are the biggest offenders. Since security has become one of the most important issues for data transfer via wired and wireless networks, many security-enhanced solutions have been created to enhance the security of data transmission over public networks. The goal of this project is to make routing safer. Proactive routing, as is well known, involves finding alternative routes and requiring packets to choose one at random from their immediate neighbors. Sending hello packets allows us to maintain track of each node's neighbors. The delivery path is then selected from nearby nodes, with the prior hop which is retained as the history node having been arbitrarily excluded. To randomize delivery channels, the proactive routing protocols DSDV and RDSDV were contrasted for various node counts. The Simulation employs this project. The rapid development of mobile computing applications and distant systems has raised awareness of quality of service (QoS) for mobile ad hoc networks (MANETs). In the MANET scenario, security is a key component of Qos provisioning. Attacks on the system could result in problems with direction, asset reservations, or even the collapse of the QoS structure if no security tool is used. In this study, two new plans will be provided from the perspectives of two alternative techniques to manage the updating of the organizational idea and allay the worries caused by interface annoyances in order to handle the security challenges of MANET Qos and the actual commitments of this investigation.

Keywords: *PDA; LAN; IEEE; Qos; MANET.*

1. Introduction

Computers are connected to each other and exchange information over wide area networks using audible electromagnetic radiation. The most common form of transmission is radio waves. The 5 GHz U NII (Unlicensed National Information Infrastructure) band and the 2.4 GHz ISM (Industrial, Scientific, and Medical) band are expected to be divided into two independent open frequencies for transmission following, with a maximum information exchange of 83 MHz each. The laws in nations with clearly defined borders outline the duties that must be upheld [1]. Comparative ideas also affect the direction and flow of energy (indoors versus outdoors). Depending on the flow control, data repetition rate, and receiving wire type used, the range of this remote radio frame can range from 10 to 100 meters to 10 kilometers. The many different receiving wire types that can be employed include omnidirectional dishes, waveguides, local radio wires, and (omnidirectional mechanical assembly). They have a 1 lm operating range and high-quality materials. In WPANs (Wireless Personal Area Networks), small devices frequently use infrared promotion, like as when a PDA is connected to a computer inside a cell [2].

IEEE 802.11 uses channel-scepter technology to sort CSMA/CA over wide area networks, which is planned to avoid collision (or perhaps to try). The CSMA/CA convention suggests that the center, after recognizing that a channel is involved, should remain committed to a sparse interface before attempting to transmit, thus choosing a personal deferral based on the content windows. Both the sender and the recipient may see what is inside the package. The related exponential backoff calculation demonstrates how the sender modifies the delay in the absence of the confirmation packet. The contention window measure is shown to have doubled for each unsuccessful attempt. Non-sent information packets are sent utilizing additional hardware. After receiving an RTS (Request to Transmit) packet from the source, the target responds by ejecting a CTS (Scan to Transmit) message upon collection. If the source successfully gets the CTS, the source sends the data packet [2].

2. Standards of frameworks

Bluetooth, HiperLAN, and the IEEE 802.11 family of protocols are just a few of the essential (3) testing for remote frameworks [3][9].

2.1. IEEE 802.11 family

The IEEE Institute of Electrical and Electronics Engineers is the organization that developed the IEEE 802.11b standard. The IEEE 802.11 FHSS (Frequency Hopping Spread Range), IEEE 802.11 DSSS (Direct succession spread range), and IEEE 802.11 IR (InfraRed) technologies use the 2.4 GHz radio channel, however they are not physically compatible with one another. Actual data transfer happens between 1 and 2 Mbps. With such accuracy, the group for whom numerous benchmarks were employed has been identified [3].

They cannot cohabit since 802.11a and 802.11b use separate frequencies. Wi-Fi, or IEEE 802.11a, operates at 5 GHz using the U-NII band division multiplexing transport technology and has a maximum information rate of 54. Where Wi-Fi, also known as IEEE 802.11b, operates is in the 2.4 GHz ISM band. The data rate will frequently fluctuate between 1, 2, and 5 Mbps depending on the hail quality. During the transmission run, the speed varied from 50 indoor meters (200 outdoor meters) for 11 Mbps to 150 indoor meters (500 outdoor meters) for 1 Mbps. Additionally, adhering to banner control is the transportation run.

IEEE 802.11g has a 20 Mbps maximum data throughput at 2.4 GHz. To guarantee compatibility with the IEEE 802.11b standard, M and DSS are included. WLANs (Wireless Metropolitan Area Networks) are anticipated to transcend LEEE 802.11's single "mit atinn" standard with IEEE 802.16n, also known as WiMAX. It only covers a small region and can only operate at frequencies between 10 and 66 GHz due to certification. The IEEE 802.16 standard was modified into IEEE 802.16a, which works in the 2-11 GHz range, to alleviate the well-known route difficulties caused by using the 10-66 GHz spectrum. Channel get to strategy a basic point in the channel get to strategies for remote frameworks is that it isn't moveable and distinguish the conveyor for package crashes meanwhile. Thusly There is no genuine method for realize a CSMA/CD (Carrier Sense Multiple Access Collision Detection) tradition, for instance, at the wire Ethernet [21].

2.1.1. Hiper LAN

The IEEE 802.11 rival Hiper LAN (High Performance Radio LAN) is a standard that has been approved by the Institute. It looks at two main categories of frameworks:

- Hiper LAN 1 has a data throughput of 10–20 Mbps and runs at a frequency of 5 GHz.
- HiperLAN 2 operates at a frequency of 5 GHz and offers a data speed of up to Mbps. Similarly, HiperMAN is a standard [5].

2.1.2. Bluetooth

Privately held companies like Agree, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, and Toshiba were among those that contributed to the development of the Bluetooth standard. A working distance of approximately 10 meters is provided by Bluetooth technology that uses the 2.4 GHz band. For instance, Bluetooth's capabilities and usability make it a good fit for compact WPANs. Furthermore, it is utilized to connect peripherals like consoles, printers, and cell phone headsets [6] [7].

3. Architecture

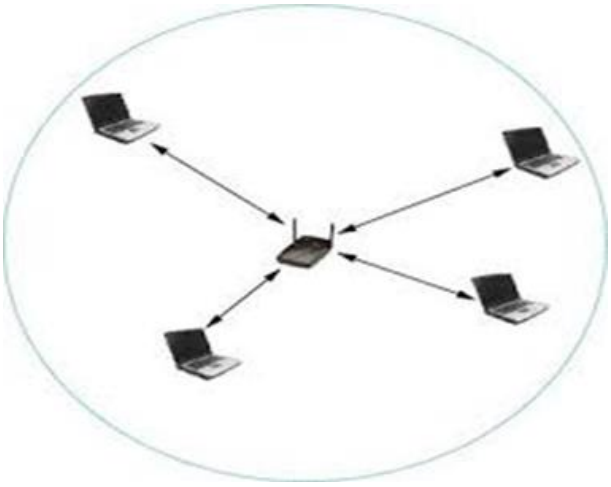

Fig. 1: Depicts A Network Cell and an Access Point Operating in BSS Mode [6].

The remote system can be configured in either BSS (Basic Organization Set) mode or IBSS (Independent Basic Service Set) mode. These two modes have an impact on the topology and flexibility of the computers (central points) that comprise the system.

3.1. BSS mode

When in BSS mode, also known as framework shape, figure 1 demonstrates how a non-versatile Access Point (AP) is remotely connected to several portable hubs. In addition to allowing users access to a networked external system like the Internet, hubs employ the AP to transport data. An ESS (Extended administration set) is developed by integrating different BSS systems [21].

3.2. IBSS mode nodes

The IBSS mode, often referred to as dispersed or impromptu shape, allows hubs to interact directly (point-to-point) without the requirement for an AP, as is depicted in figure 2. There is no solid foundation. In order to communicate, hubs must be close to one another [21].

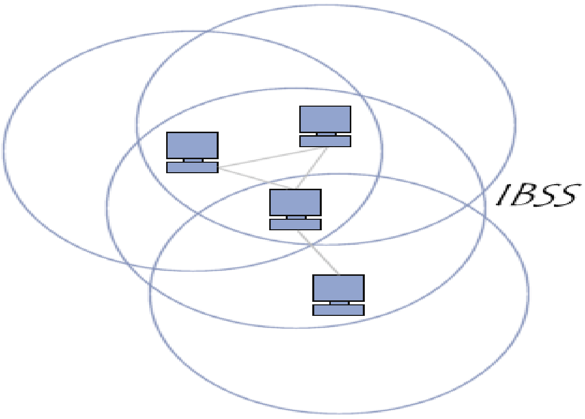

Fig. 2: IBSS Mode [7].

3.3. Ad Hoc network

A specially appointed system, or MANET (Mobile Ad hoc NET Work), is a system made just out of hubs, there isn't an access point here. There is constant connection between the rods. In fact, an extraordinarily selected framework has the capacity of impacting correspondences maybe to even among two center points that are not in arrange transmission reach out with each other: packs to be exchanged between these two centers are sent by widely appealing centers, using a directing computation. Along these lines, a MANET may spread on greater detachment, gave that its terminations interconnected with a series of associations among center points (furthermore called switches of this outline). In the uniquely selected framework [4][21].

An in outstanding of uniquely delegated framework, made out of outfitted with sensors screen temperature, sound. These contraptions are regularly passed on in far reaching number and have compelled resources to the extent essentialness, memory, and computational power win un network offers in portent central focuses with respect to:

- As long as they are still within radio range, it is widely considered that a remote framework enables machines to be fully adaptive.
- A remote system makes it easier to keep connections between equipment when close contact to one another is not required. Following that, setting up a remote system is easier and quicker. It may occasionally be challenging or uncomfortable to carry links, such as front lines, search-and-rescue missions, or regular communication requirements, in historic structures, open shows, preparation stations, or burial site locations due to the topography and surroundings.
- The initial cost of a small remote system (the cost of system cards) may be higher while growing a wired system is typically less expensive. Since there are no cables, there are no setup, material, or maintenance expenditures. The topology of a remote system can also be easily changed by adding or removing machines.

Then again, there are a few disadvantages that should be pandered:

- Using a customized transporter with a different sense of access (CSMAI convention) can help with hidden and exposed terminal issues.

4. Related works

Due to its enticing lack of infrastructure, wireless ad hoc networks are of particular interest to researchers in both the academic and industrial sectors. The demand for conventional networks to enable multimedia applications has highlighted the significance of qos provisioning for wireless ad hoc networks, making it a highly desirable objective. Technically speaking, because of mobility, a shared wireless medium, and dispersed multi-hop communications, QoS provisioning in wireless ad hoc networks is challenging [10].

4.1. Security is important

Mobile ad hoc networks have features like rapid topological changes, no fixed infrastructure, and high node mobility. These qualities make ad hoc wireless networks more vulnerable to malicious assaults than the open Internet. The majority of the vulnerability is explained by the following factors [10].

- The network is vulnerable to assaults ranging from passive eavesdropping to active interfering due to the utilization of wireless connectivity. It differs from standard wired networks in that there are no physical cables to access or several defined lines to traverse at the gateway.
- Independently moving mobile nodes are more prone to kidnapping, hostage taking, and hacking. It may be difficult to pinpoint a single mobile node in a large-scale ad hoc network, making attacks by a compromised node within the network considerably more disruptive and difficult to pinpoint. Since byzantine failure could make it more difficult for peer nodes to acquire and maintain confidence, it should be avoided.
- Adversaries may use this weakness for new kinds of attacks aimed at disabling cooperative algorithms because the ad hoc network lacks centralized operations and many algorithms depend on the cooperative engagement of all nodes.
- Unlike a wired network, where routers and gateways may be protected, most ad hoc routing algorithms are cooperative in nature. A malfunctioning node may render the entire wireless network inoperable as a result of providing incorrect routing information.

4.2. Service excellence

Quality of Service (QoS) is a general term used to assess any technology's usefulness from the viewpoint of the user. Quality of service (QoS) in computer networks refers to the incorporation of techniques to control network activities like transmission and error rates in order to achieve a specific level of service. The main goal of QoS provisioning is to provide more predictable network behavior so that network information can be delivered more consistently and network resources may be used more effectively.

A number of quantifiable, pre-specified service criteria, such as minimum bandwidth, maximum latency, maximum delay variation (jitter), maximum packet loss rate, etc., can be used to characterize network services. According to the rules of the agreement, the network must make sure that the user's service requirements are satisfied throughout the flow (a packet stream moving from the source to the destination) after accepting a service request from the user. In order to provide a flow, the network must provide a variety of service guarantees.

4.3. Quality of service (QoS) is essential

The different QoS restrictions are separated into: Limitations on time (Delay, Jitter): The limitations cover matters like reliability, regularity, and physical space. Other limitations include the system buffer, network/system bandwidth, and error rate. Different applications require varied levels of network performance depending on their bandwidth needs and sensitivity to delay. A general overview of the bandwidth and latency sensitivity requirements for various applications is provided by Figure 3. As can be observed, bandwidth needs increase as latency sensitivity increases. High packet counts for jitter and delay are typical on data networks. Depending on the needed email bandwidth, response times for FTP uploads are typically in the range of a few seconds to hours [11].

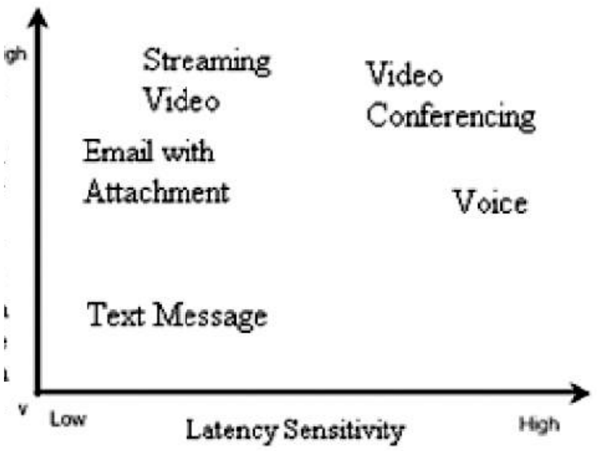

Fig. 3: Shows the Requirements for Various Applications and Networks.

Table 1 illustrates how the traffic patterns and QoS requirements of various applications vary. Since data is delivered in incredibly short batches, electronic mail ISMTF, file transfer (FTP), and remote terminal (Telnet) have very low bandwidth requirements. Since data is delivered in a series of rapid bursts, the bandwidth needed to visit HTML webpages varies. Applications that stream video need a lot of bandwidth and are especially prone to jitter and latency [11].

Table 1: Traffic Behavior and Qos Requirements [21]

Applications	Traffic Behavior	QoS Requirements
Electronic Mail (SMTP) File Transfer (FTP) Remote Terminal (Telnet)	Traffic Behavior Small, batch file transfers	QoS Requirements Very tolerant of delay B/W requirement: low Best Effort
HTML Web Browsing	Serial of small, bursty file xfer	Tolerant of moderate delay B/W requirement: varies Best Effort
IP-based Voice (VolP)	Constant or variable bit rate	Very sensitive to delay/jitter B/w requirement: low Requires predictable delay/loss
Streaming Video	Variable bit rate	Very sensitive delay? Jitter B/w requirement: High, variable Requires predictable delay? loss

4.3. Qos in-situ networks in wireless

The following characteristics of Quality of Service have a significant impact on the QoS design and routing algorithms used in MANETs: In the center of the network, the Core System's mechanics are in operation. The routers are necessary for the QoS delivery. The two techniques that core systems employ are scheduling and queue management. When a packet must be discarded, queue management is employed to make the decision. Instead of being a point-to-point link like in wired networks, the link between two nodes is a shared medium [10] [20].

4.4. QoS routing protocol design considerations

As a result of MANETs' very restricted network resources, QoS routing can only be implemented with limitations on bandwidth, latency, jitter, packet loss rate, and route stability. Ad hoc QoS control issues are impacted by the following MANET features:

Since the bandwidth for shared media is periodically unavailable, resource reservations are unreliable. As a result of the link's unpredictable capacity, entry limitations are difficult. Large changes in node communication capability may lead to routing recovery or QoS redirection, as was already mentioned [20].

In the study that is provided, Hammoudeh, M., and Newman, R. give a comprehensive analysis of the issue and the current QoS routing algorithms in wireless ad hoc networks [12]. In his paper, he looks at the shortcomings of existing routing algorithms, such as how they fall short of the standards for wireless ad hoc networks (such as high fidelity, little overhead, scalability in a wide network, capacity for QoS routing, etc.). The global state routing (GSR) method should be used. GSR maintains a global view of the network architecture while basing local routing decisions on the connection status vectors shared by nearby nodes. Depending on how close a node is to the destination, connection status vectors are exchanged more often. The control message is kept to a minimum by this multi-level fractal scope method, which lowers bandwidth consumption [20].

A bandwidth routing strategy was given by Faheem, Tuna, and Gungor [13] to achieve QoS in multi-hop mobile networks. The protocol has features for computation and bandwidth distribution throughout. The bandwidth and QoS available to each destination in the mobile network are known to the source. Knowing this enables real-time apps to be properly enabled and allows for the right deployment of QoS communications inside the mobile network. The leaflet also includes information on the connection to the ATM [20].

5. Security mechanism

When the target center needs to know the path there, it sends RREo packets to the system. The hub that sent the RREQ packet transmits it to hubs nearby, who then send it to their own neighbors. The center of the road axis can follow a number of distinct reversed trajectories; it normally selects the one that calls for the fewest back checks. Customers can request a deviation from the predetermined distance vector by using the wrapper (AODV routing agreement) that we offer. To ensure that the pertinent data is transferred between the source and the destination, we have created a method [14].

When the hub receiving the request is either aware of a sufficiently new path to the target or is the target itself, an RREP packet is constructed and sent along the switching route in the direction of the initiating hub. In this case, the REQ generator will modify its routing table. Since it contains the greatest "lagging" routing data, it uses the cycle with the best order number for the target [15] [20].

6. The solution

Our proposed strategy: Each core in the system is required to attach these extensions to its IP address in every RREQ packet it transmits. The hub accepting the package checks to confirm its source by including the added person's extension and handing over the known source IP to it to get each one. A malicious core in the system does not realize that it needs to attach its own extension to its address and thus any packet from these modes drops its neighbors, communicating with the entire system, warning every one of the hubs in the system of the proximity of the retaliatory core and its IP address, saving processing time [16]. Like any hub, any package from the malicious center can get rid of it easily without any additional examination. In this way the malicious hub is disconnected from the system. In addition to the free IP address, we also install TIMER on each node. The timer begins when a node transmits an RREQ packet and ends when that same node gets an RREP packet. The timing value thus offers an estimation of how long it will take a nearby node to deliver a route reply [17]. The IP address does not match and the timeout value is lower than it would be for a conventional node since black holes respond quickly without examining the routing database or the complement of their IP address. However, the timer value will also be displayed when the destination node is closer to the source node. To avoid this, the timing value is compared to the threshold value.

7. Simulation parameter

Table 2: Simulation Parameters

Simulation Time	10 Min
Bandwidth	3 Mbps
Frequency of Operation	2.6 GHz
Simulation Area	1500 m 1500 m
Number of Nodes	60
Offered Traffic	14 packets sec
Radio Range	260 meters
Application	CBR
Transport	AODV
Network	802.11

Using GloMosim, mobile hubs choose a target from an unpredictable waypoint show [19], proceed along an unimpeded path, and evaluate the effectiveness of the suggested security display.

1) Average throughput: This directing skill metric is built using the ratio of information packets delivered to objectives to information packets originated by sources.
2) End-to-end delay: This is the amount of time that passes between the source hub sending the first message and the goal hub receiving the last message in the system.
3) Control overhead: The overall number of control bundles sent by each hub throughout the replay.

7.1. Simulation results

The accompanying figures outline the execution consequences of information security as for different parameters acquired utilizing GloMosim by the continuous course disappointments, which in tum expands the quantity of course disclosure process.

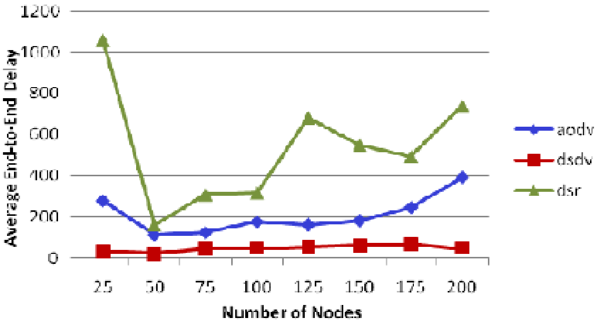

Fig. 4: Standard End-to-End Relation between Delay and Node Count.

Figure 4 outline the ordinary end-to-end delay at the data mixed arrangement, which is described to be the inward between the tune when a source center begins the data package and the time when the objective center gets the last data distribute. From the outline, we watch that an adaptability manufactures the concede increases, fundamentally due to the retransmission of information bundles in view of course disappointments.

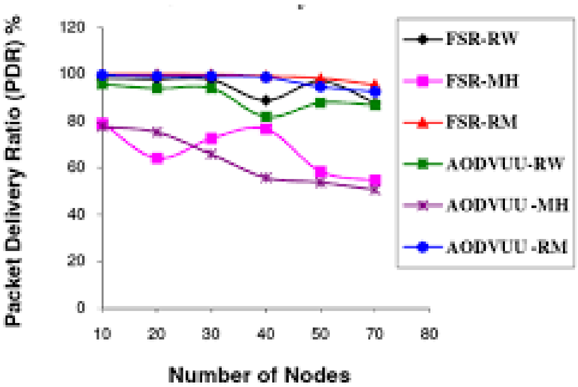

Fig. 5: Packet Delivery Ratio and Nodes: A Relationship.

The execution of the package conveyance% under various portabilities is shown in Figure 5. The graph demonstrates that even at low versatility, as the number of hubs rises, the whole encoded information bundles are efficiently sent. When the number of hubs increases because to natural disappointments, there is very little information bundle loss for medium portability scenarios, but for low portability situations, the system with high flexibility loses around 8% to 10% of information bundles as the number of hubs increases. This is mostly because of a pattern of course failures and a delay in bundle termination brought on by the delaying of the encryption and unscrambling process.

8. Conclusion

The aforementioned method takes into account the stability of the network from all perspectives. Two distinct factors have the potential to reduce the network's lifespan. First, a node moving beyond of the radio range may result in a loss of connectivity. Second, the network may fracture as a result of a node's energy loss. Based on these two criteria, the suggested method's metric assesses the stability of the network. The pathways that result from the various routing decisions made at each node are known as node disjoint paths. By doing this, we try to avoid quickly depleting every node along a single path. Therefore, it is anticipated that this method would result in node disjoint pathways that are incredibly stable, reliable, and resilient. Since the pathways are node separated, the rate of energy loss is accelerated.

References

[1] Hackmann, G., Sun, F., Castaneda, N., Lu, C., & Dyke, S. (2012). A holistic approach to decentralized structural damage localization using wireless sensor networks. *Computer Communications*, *36*(1), 29-41. https://doi.org/10.1016/j.comcom.2012.01.010.

[2] Park, P., Ergen, S. C., Fischione, C., Lu, C., & Johansson, K. H. (2017). Wireless network design for control systems: A survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 978-1013. https://doi.org/10.1109/COMST.2017.2780114.

[3] Adjih, C., Minet, P., Muhlethaler, P., Baccelli, E., & Plesse, T. (2008). Quality of service support, security and OSPF interconnection in a MANET using OLSR. *Journal of Telecommunications and Information Technology*, (2), 70-76.

[4] Sridhar, S., & Baskaran, R. (2015). Efficient Routing in Mobile Adhoc Networks Emphasizing Quality of Service by Trust & Energy based AODV. *Journal of Communications Software and Systems*, *11*(1), 1-7. https://doi.org/10.24138/jcomss.v11i1.111.

[5] Karakus, M., & Durresi, A. (2017). Quality of service (QoS) in software defined networking (SDN): A survey. *Journal of Network and Computer Applications*, *80*, 200-218. https://doi.org/10.1016/j.jnca.2016.12.019.

[6] Singh, B., Rana, H., Verma, A., Duhan, A., & Zayed, M. (2016, February). SRR loaded microstrip patch antenna for Bluetooth, HIPERLAN/WLAN and WIMAX. In *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 34-37). IEEE. https://doi.org/10.1109/SPIN.2016.7566658.

[7] Coutras, C. (2015). Priority Levels in a HIPERLAN Based Forwarding Mechanism for Intermittent Connectivity. *ICN 2015*, 13. 8-. Z. Hass & R. Pearlmann, "Zone routing Protocol"(1999), IETF Internet Draft.

[8] Akin, E., & Korkmaz, T. (2019, January). Comparison of routing algorithms with static and dynamic link cost in SDN. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-8). IEEE. https://doi.org/10.1109/CCNC.2019.8651815.

[9] Asif, M., Khan, S., Ahmad, R., Sohail, M., & Singh, D. (2017). Quality of service of routing protocols in wireless sensor networks: A review. *IEEE Access*, *5*, 1846-1871. https://doi.org/10.1109/ACCESS.2017.2654356.

[10] Jiwon Park, Sangman Moht & Ilyong Chung (2008),” Multipath AODV Routing Protocol in Mobile Ad Hoc Networks with SINR-Based Route Selection”, International Symposium on Wireless Communication Systems, IEEE, pp:682-688. https://doi.org/10.1109/ISWCS.2008.4726143.

[11] Hammoudeh, M., & Newman, R. (2015). Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance. *Information Fusion*, *22*, 3-15. https://doi.org/10.1016/j.inffus.2013.02.005.

[12] Faheem, M., Tuna, G., & Gungor, V. C. (2017). QERP: Quality-of-service (QoS) aware evolutionary routing protocol for underwater wireless sensor networks. *IEEE Systems Journal*, *12*(3), 2066-2073. https://doi.org/10.1109/JSYST.2017.2673759.

[13] Shrivastava, A. K., Vidwans, A., & Saxena, A. (2013, September). Comparison of AOMDV Routing Protocol under IEEE802. 11 and TDMA Mac Layer Protocol. In *2013 5th International Conference and Computational Intelligence and Communication Networks* (pp. 117-122). IEEE. https://doi.org/10.1109/CICN.2013.35.

[14] Kanakala, S., Ananthula, V. R., & Vempaty, P. (2014). Energy-efficient cluster-based routing protocol in mobile ad hoc networks using network coding. *Journal of Computer Networks and Communications*, *2014*. https://doi.org/10.1155/2014/351020.

[15] Wang, Z., Bulut, E., & Szymanski, B. K. (2009, June). Energy efficient collision aware multipath routing for wireless sensor networks. In *2009 IEEE International Conference on Communications* (pp. 1-5). IEEE. https://doi.org/10.1109/ICC.2009.5198989.

[16] Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the Internet of Things: A context-aware and multi-service approach. *Computers & Security*, *39*, 351-365. https://doi.org/10.1016/j.cose.2013.09.001.

[17] Krishna, P. V., Saritha, V., Vedha, G., Bhiwal, A., & Chawla, A. S. (2012). Quality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks. *IET communications*, *6*(1), 76-83. https://doi.org/10.1049/iet-com.2010.0763.

[18] Ni, M., Zhong, Z., & Zhao, D. (2011). MPBC: A mobility prediction-based clustering scheme for ad hoc networks. *IEEE Transactions on Vehicular Technology*, *60*(9), 4549-4559. https://doi.org/10.1109/TVT.2011.2172473.

[19] Lu, B. (2005). *Quality of service (qos) security in mobile ad hoc networks*. Texas A&M University.

[20] Benamar, K. A. D. R. I. (2007). The adaptation of security mechanisms for Ad hoc Networks. *Unpublished Master Thesis, University of Abou Bekr Belkaid, Algeria*.