Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Energy Consumption Analysis of Iot-Manet Based Systems with Anova Assessment for Tackling Covid-19

Ashu Gautam*

*Corresponding author, Department of ECE, MRIIRS, Faridabad, India 121001. E-mail: ashuone@gmail.com

Rashima Mahajan

Department of CSE, MRIIRS, Faridabad, Inida,1210011. E-mail: rashima.fet@mriu.edu.in

Sherin Zafar

Department of CSE, SEST, Jamia Hamdard, New Delhi, India 110062. E-mail: zafarsherin@gmail.com

Abstract

The epidemic situation generated as a result of COVID -19 crossways the sphere observed the practices of various emerging technology like Internet of Thing (IoT) along with norm of dynamic fields. The wireless communication based on networks such as wireless mesh networks (WMN) and Mobile Ad-hoc networks (MANETS) proven to be very successful for monitoring of patients remotely. The MANET protocols that are simulated in this study are Ad-hoc On Demand Vector (AODV), Secure AODV (SAODV) and Hybrid Wireless Mesh Protocol (HWMP). In this investigation work, most appropriate routing protocols to knob DDoS attacks are simulated using NS-2 and assessed in terms of average energy consumption in the state of changing speed connections among devices called mesh nodes. Further ANOVA test is utilized for further accessing for the best suited routing protocol for handling the data packets, which is HWMP , considerable less susceptible for DDoS assaults dominant in healthcare field.

Keywords: COVID -19; AODV; SAODV; HWMP; DDoS attacks; Energy consumption; ANOVA; IoT-MANET; e- Healthcare sector.

DOI: https://doi.org/ 10.22059/jitm.2022.86485 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received January 12, 2021 Accepted March 25, 2021

Introduction

The coronavirus led to a powerful negative impact on the economy, lifestyle across the globe. With lack of food, transportation and health related facilities are further adding a fuel in burning situation across 170 countries as reported by WHO (World Health Organization(Agrawal ,2014). At this point of time its becomes really important to break the conditions created in this pandemic, many researches have concluded to control this situation one of the most important step is to measure the impact of this deadly virus. Thus monitoring of symptoms is playing a key role to overcome from this current situation. It has been reported by many researchers that IoT (Internet of Thing) is proven to be the most important pillar in process of recovery and to a great extent has helped patients for speedy recovery of health(Gautam, Mahajan& Zafar,2021) .The countries of APAC (Asian Pacific and Australian Countries) have a tremendous usage from IoT based technology for keeping the things under control and by 2023 there is going be surge of almost 253 billion USD investment in health sector related apps and devices to monitor the vital characteristics of the infected person(Islam et al.,2015). In many social media sites it has proven fact that devices like drones are helping a lot in monitoring the particular sector of a crowded place, also they are helpful in distributing the food, medicines to patients in the hospitals, where the movement of other health professionals is not possible due to limited staff and nature of disease(Yadav & Agrawal,2018). Many health related apps are helping under lockdown time period also the symptoms of the patients could be sent via apps for remote monitoring or for taking suggestion from doctor. Thus remote monitoring plays a vital role in monitoring the conditions of the patients in urban as well as rural areas where movement is not possible. This has become possible only due the advancements in the wireless network technology and its amalgamation with IoT. This present paper contributes in making utilization of the best routing protocol for fast delivery of data from patient to the doctor in terms of QoS parameter for the simulation world carried on NS-2.

MANET – IoT

The COVID-19 situations emphasized upon remote monitoring of various health parameters of symptoms as well as too make sure the social distancing is being followed for handling the pandemic. The sensors plays a crucial role in monitoring the conditions which forms the part of the WSN .These sensors could be of wide range for measuring the temperature, pulse, oxygen level etc as per the recommendation of healthcare professionals. Also the smart devices like smartphones which are equipped with many sensors due to the advancements in the embedded technology. The IoT device is basically any device connected with internet along with some computational power. Thus (Figure 1) the black nodes inside the circle explains the various smart devices which could be wearables ones like that of smart watches or wrist bands, recording our symptoms and sending these signals from one point to another either via wired technology or wirelessly through gateways Thus the wireless local area networks (WLAN) and MANET have to connect to internet to send the information of the important vital parameters. Such networks when exposed to Internet are influenced by different types of attacks which have been categorized as active and passive attacks in many of the research work carried in different researches. The chief cause for these attacks is the transitional medium, which is complete wireless access along with reticent assets. Therefore the infrastructure and various resources of such networks became unavailable for the actual users due to the susceptible nature of networks to various kinds of attacks (Brill & Nash, 2017).

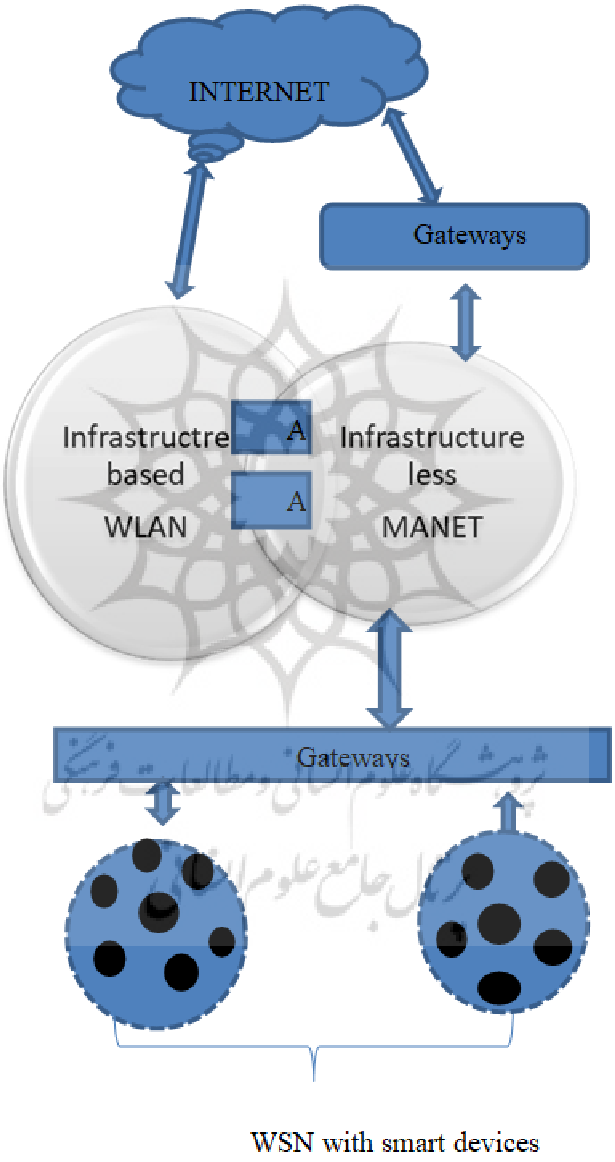


Figure1. Architecture for MANET –IoT Networks

To places where network connection is an issue MANET have proven their worth for sending information from inaccessible points and has been reported by various researches specially to the military people engaged in the disaster monitoring during war ,earthquakes and many similar circumstances etc for sending data from one smart gadget to another., far off from the radio range. Thus to make the communication reliable for remote monitoring of data, routing ability is important for successful transmission of end-to-end data transfer. For finding best route for sending data many protocols were studied in different researches carried over last decade majorly and majorly focusing upon reactive ,proactive and hybrid techniques for networks. The merging of MANET and WSN, indicates that MANET is appropriate to be integrated with the Internet of Things (IoT) for various applications (Gautam, Mahajan & Zafar, 2020), (Cai et al.,2020).

Security challenges in IOT- MANET based networks

The previous section reflects the usage of MANET in layered architecture for IoT based environment. The security issues in MANET based networks can be broadly classified active and passive threats. The other criteria for classifying routing protocols in MANET are uniformity and non-uniformity of protocols completely depending upon the mobile nodes role in routing. Mobile node possessing same functionality, significance and the role forming uniformity of the protocol used used in MANET based environment and characterizing with as reactive nature or proactive one. (Figure 2)While the network in which mobile nodes (Alharbi, Aljuhani, & Liu,2018) have distinct function or significance forming non uniformity of protocols and various researchers have proposed the classification of such routing protocols (Khalaf & Abdulsahib,2020).

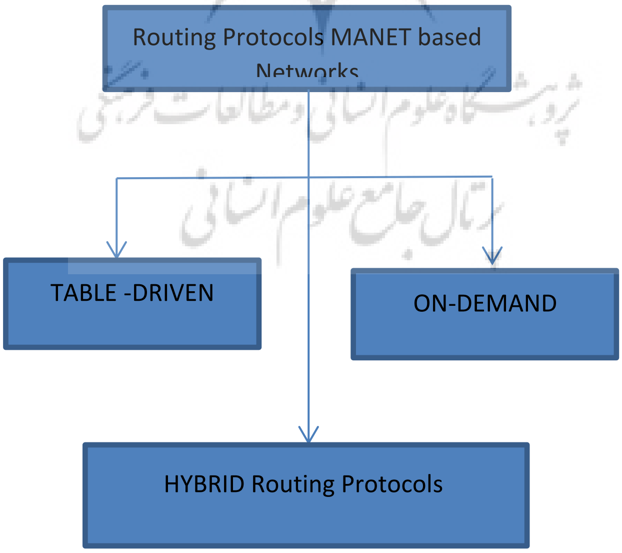


Figure2. Routing Protocol Classification in MANET based networks

The communication held between two IoT devices is analogous to the routing of data among MANET nodes. The nodes are actually the smart IoT devices which are attached the patient for picking up the data of various parameters. Therefore all the different types of routing protocols sown in (Figure 2) are applicable for the IoT MANET based environment. The table driven is famously known as proactive, and on–demand is reactive category of routing protocols. Abundant arrangements for MANET routing subsists, with extensive reviews cited in (Cogliati et al., 2018). The amalgamation of nodes of IoT in MANETs and vice versa i.e. IoT gadgets attached to nodes of MANET have by standard IP(Internet Protocol) connection with Internet. This amalgamation makes the MANETs characteristically low power and lossy networks (LLNs).

The (Figure 3) represented the classification of the attacks in routing protocols of low power lossy networks on the basis of confidentiality and integrity and secondly on the availability. Among all the RPL attacks black hole attack and neighbor attacks comes under both criteria's (Aldana et al., 2020). The multiple replicated individualities of legitimate nodes of network nodes are used by malicious devices or nodes for compromising routing ultimately making them unapproachable in sybil assaults. The disruption of routing topology and data flow rate of traffic is made by wormhole assault. This wormwhole attack is accomplished by two malicious nodes, playing among themselves by forwarding the data packets among each other. The main objective of one other category of attack called flooding assault is to exhaust the battery power (Chelli, 2015).

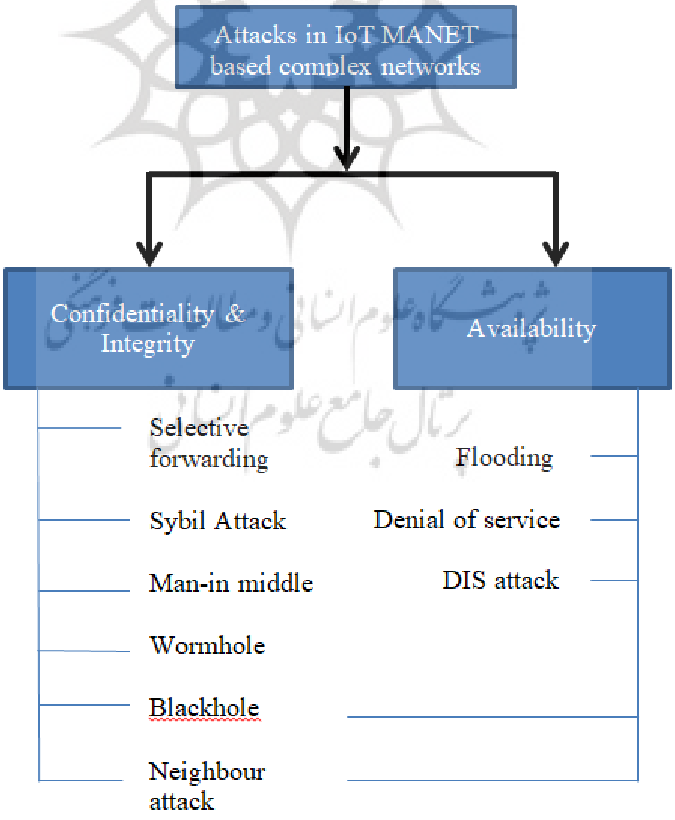


Figure3. Security Aspects in Complex Networks

In man-in-the middle assault, empirically inappropriate messages are addressed to the receiver. In this sort of assault messages may take either category of a false negative or a false positive (Jain & Tokekar, (2015). This may lead the operator to initiate unnecessary activities, such as breaker flipping, when it is not essential, or may also lead the operator to consider everything to be okay and therefore not to captivate an action when action is needed(Sharma & Trivedi, (2016).

Adhoc networks are extremely susceptible to distributed denial of service (DDOS) assaults (Singh & Singh, 2019). Such DDOS occurrences put away all the resources of system such as power of battery ,consumption of bandwidth, more energy consumption along with machine cycles of CPU etc .Further such attacks make assets or smart devices called nodes inaccessible to genuine users. The dynamic characteristics of mobile nodes smart phones in the considered scenario along with the topology of the MANET based environment makes them prone to these DDOS assaults causing the packet dropping while transmission. Many researchers suggested different routing protocols for the handling such attacks, but none could conclude the best routing protocol for among the existing reactive ,proactive and hybrid ones in adhoc networks(Kumari, Singh & Manjul,2020). In this research work, we are comparing the three routing protocols most widely proposed for handling data, under the influence of SYN flood attacks, which is one of the categories of DDoS assaults (Walikar & Biradar, (2017).

Introduction segment of the investigation paper has focused on impact of COVID -19 and concepts of networks and its vulnerability for various attacks in healthcare sector. Further relevant analysis has been done on the various routing protocols used in end to end transmission care sector based on MANET. The subsequent discussion is explaining the simulation model comprising the scenarios considered in simulation model for carrying the research work. The results centered on energy consumption as Quality of Service (QoS) parameter followed by ANOVA test for validification of variance among three routing protocols. The discussions and conclusion on the investigation work carried out is mentioned in research paper ,which is followed by future work of study and references are listed in the end.

Routing Protocols

The routing protocols helps to send the data from one end to other end in mobile adhoc networks [16]. The steadily expanding utilization of the web particularly during pandemics has prompted more noteworthy sharpness and consideration in upgrading the security of organizations alongside methods of directing by different scientists. For accomplishing the determination of best routing protocol, the metrics used is Quality of Service (QoS) parameters (Sanzgiri et al., (2002). In the work the researchers focused on comparing the three routing protocols for jitter ,delay ,throughput under scenario of varying number of nodes .The best commonly used reactive protocol is Ad Hoc On-Demand Distance Vector (AODV)

,as it shows and maintains paths only on demand .The exclusive feature of AODV is dynamically formation of entries of routing table.Also all the entries of table gets expired if they not in use

Secure AODV (SAODV) is more secured version of AODV with incorporation of an extension in different AODV formats of packets .Mostly digital signature are incorporated for shielding the non-mutable info in packets along with hash chains for protecting the mutable information for example hop count. Similar to AODV, SAODV too have two different mechanisms one for discovering route and second for maintenance of route. The chief difference between AODV and SAODV is the presence of more complex process for detection of route because SAODV upsurges the course of directly authenticating the endpoint node with the help of random numbers exchange (Siwach, Sehrawat & Singh (2020).

The third category of MANET routing protocols utilizes both on demand and table driven strategy and are called as Hybrid protocols due to presence of characteristics of proactive and reactive types of routing protocols for attainment of enhanced effects[22]. Such protocols exercise reactive routing in determining the route, while proactive feature is used in the maintenance of table. Although many researchers researched on several sorts of hybrid protocols being most famously utilized for discovering routes reported in their work for Adhoc networks. In one (Gautam, Mahajan & Zafar,(2019)work has been proposed to compare the three routing protocol for PDR and delay under the scenario of varying nodes .In this present research work three routing protocols have been compared for energy consumption while transferring the data in the scenario of varying speed among 30 fixed nodes.

Results and discussion

This study work is realized while utilizing mobility model for comparing most widely used hybrid, secured and reactive routing protocols. One of the important aspects for analysis is to analyse the impact of attacks of the performance of adhoc based complex networks. In this research study instead of varying the number of nodes, the comparison is based on the changes in speed variations, keeping number of nodes fixed. It is one of the significant characteristic of ad-hoc networks to form a network in varying speed scenario. Simulation setting setup for mobility based model with varying speed among fixed nodes on HWMP, SAODV and AODV is shown above in (Table 1).The number of nodes considered fixed in this case is 30.

Table1. Simulated environment with respect to changing speed among fixed 30 nodes

Parameters	Value Used
No. of Nodes	30
Area Traffic	1800 x 840 Constant Bit Rate
Simulation Time	60 Sec
No. of Connections Traffic Rate Speed	20 4 packets/s 10,20,30,40,50 m/s
Packet Size	1024

Energy consumption is one of the most important parameters for the design of IoT – MANET system. It is highly recommended to search for the routing protocols, having minimum energy consumption. Since most of the health app are part of the tools used against fighting COVID-19 and are widely used by masses through smartphones.

The (Table 2) reflects the energy consumption comparison among routing protocols considered in work. (Figure 4) represents the bar graphs whereas (Figure 5) and (Figure 6) are graphs for energy consumption variation for three protocols in nonappearance and in presence of DDoS attacks respectively.

Table 2.Variation of energy consumption with varying speed for fixed 30 devices as nodes for three routing protocols

Routing Protocols	Energy consumption for varying speed for fixed 30 nodes (10,20,30,40,50)				
	10	**20**	30	**40**	**50**
AODV without Attack	1982.38	2155.07	2265.29	2407.76	2527.42
AODV with Attack	2318.49	2564.53	2738.31	2908.83	3013.82
SAODV without Attack	1837.66	2091.54	2183.18	2278.41	2304.72
SAODV with Attack	2011.35	2256.9	2437.86	2609.27	2765.86
HWMP without Attack	967.71	1099.35	1239.02	1542.38	1784.81
HWMP with Attack	1876.86	2109.82	2317.27	2462.21	2598.73

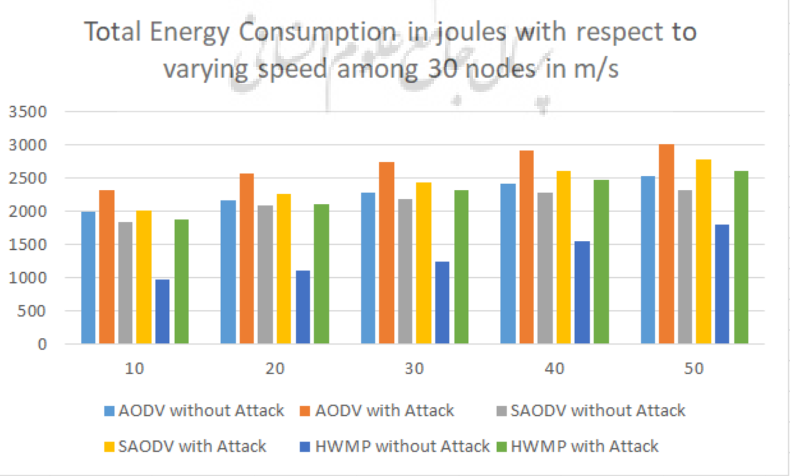


Figure 4. Bar Graph based assessment of total energy consumption in three protocols with changing speed connection among 30 nodes

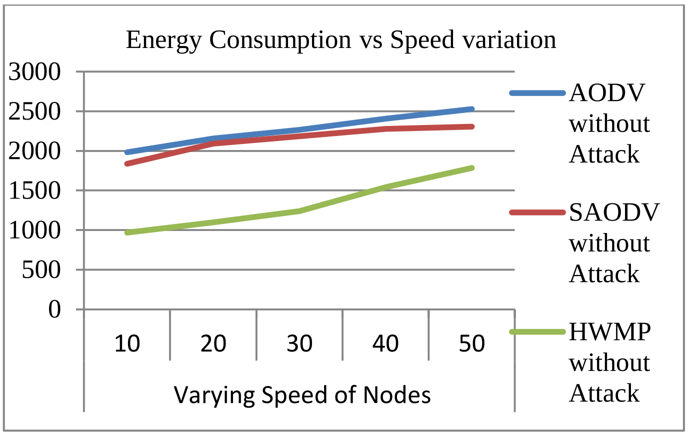


Figure.5 Energy Consumption in absenteeism of DDoS assaults for protocols with varying speed connection among 30 nodes

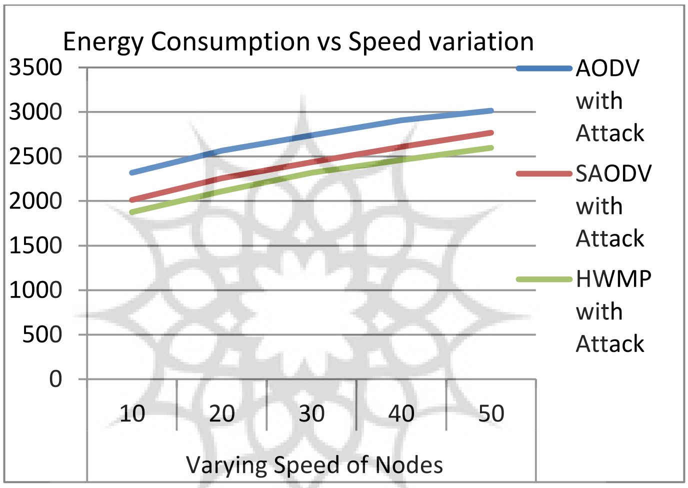


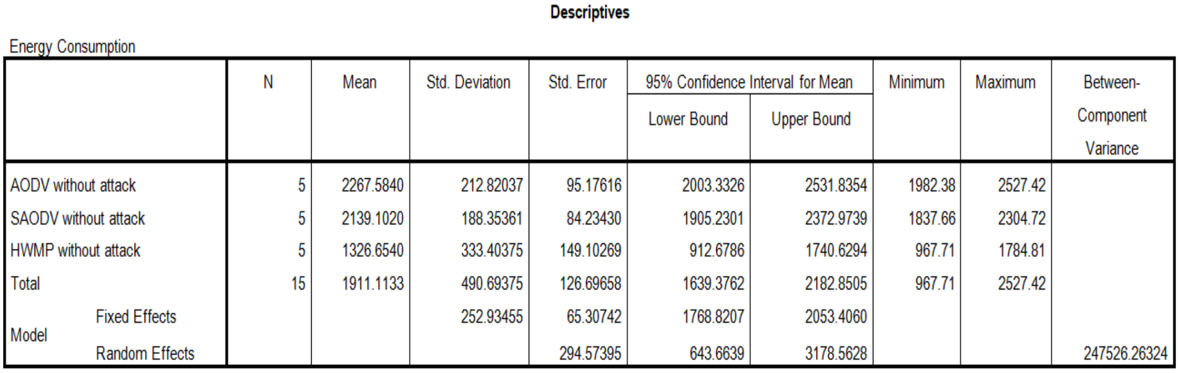
Figure.6 Energy Consumption under influence of DDoS attacks for three routing protocols with varying speed connection among 30 nodes

For 50 m/s, HWMP is 41.6% better than reactive category (AODV)and 29.12% improved than SAODV, in nonappearance of DDoS assaults . Under the influence of attack for 50m/s speed among 30 nodes, HWMP is 15.97% and 6.43% improved from AODV and SAODV, correspondingly. Thus, HWMP reasonably delivers improved outcomes than AODV and SAODV, therefore can be concluded that hybrid protocol HWMP is much more advantageous to be employed in patient healthcare environs.

One Way ANNOVA Test

In this research study we used the statistical tool of IBM –SPSS for understanding the variance within the routing protocols analyzed and also to know the variation among each other with respect to the varying speed of connections among 30 nodes. Since the number of routing protocols simulated in NS-2 for this research study was three hence we are using ANOVA test which is used for analysis of variance among more than 2 group. Thus the degree of freedom k>2 so we applied the ANNOVA test with (α=0.05).

Table 3. Descriptive for three routing protocols in absence of attacks for energy consumption



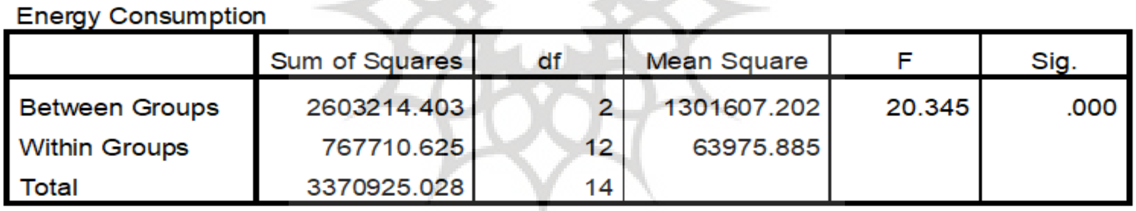
Descriptives

Energy Consumption

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum	Between-Component Variance
						Lower Bound	Upper Bound			
AODV without attack		5	2267.5840	212.82037	95.17616	2003.3326	2531.8354	1982.38	2527.42	
SAODV without attack		5	2139.1020	188.35361	84.23430	1905.2301	2372.9739	1837.66	2304.72	
HWMP without attack		5	1326.6540	333.40375	149.10269	912.6786	1740.6294	967.71	1784.81	
Total		15	1911.1133	490.69375	126.69658	1639.3762	2182.8505	967.71	2527.42	
Model	Fixed Effects			252.93455	65.30742	1768.8207	2053.4060			
	Random Effects				294.57395	643.6639	3178.5628			247526.26324

(Table 3) above illustrates s the descriptives for AODV, SAODV and HWMP ,which includes the total terms in particular routing protocols denoted by N ,Mean of individual routing protocols along with standard deviation .(Table 4) below demonstrated the ANOVA test held on three routing protocols which inludes the information of degree of freedom F critical and .There is five step procedure for the conducting and analyzing the ANOVA test. The ANNOVA hypothesis test is shown in (Table 3) and (Table 4).Since the $F_{critical}$ is 0.000 so we reject the null hypothesis H_0 which says that $\mu_{1=}$ $\mu_{2=}$ $\mu_{3.}$

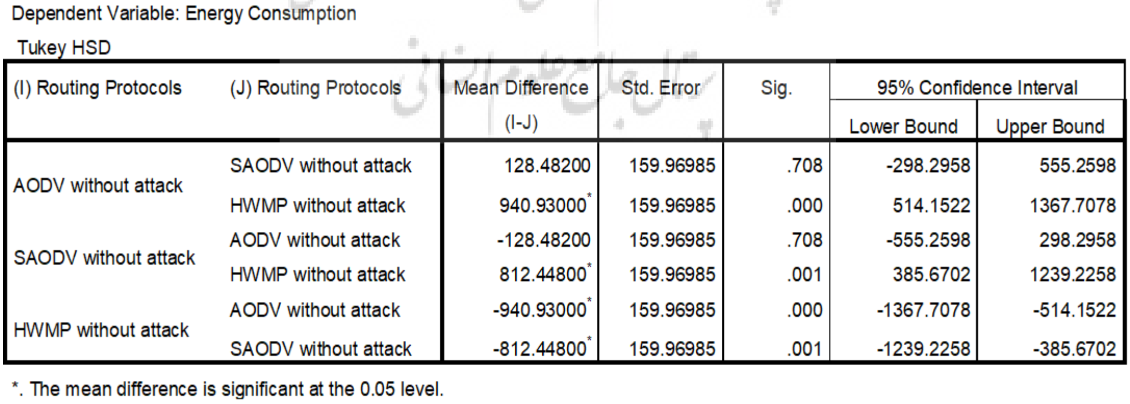
Table 4. ANOVA test for three routing protocols in absence of attacks



Energy Consumption

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2603214.403	2	1301607.202	20.345	.000
Within Groups	767710.625	12	63975.885		
Total	3370925.028	14			

Table 5.Multiple Comparisons for three routing protocols in absence of attacks



Dependent Variable: Energy Consumption

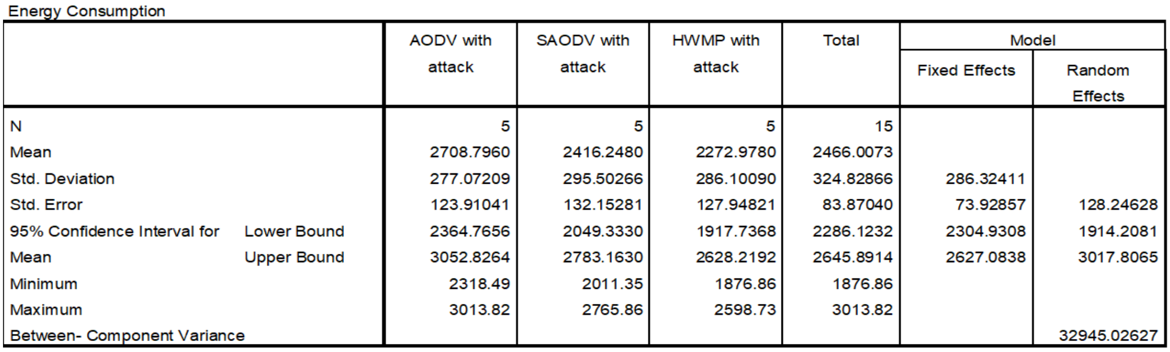
Tukey HSD

(I) Routing Protocols	(J) Routing Protocols	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
AODV without attack	SAODV without attack	128.48200	159.96985	.708	-298.2958	555.2598
	HWMP without attack	940.93000*	159.96985	.000	514.1522	1367.7078
SAODV without attack	AODV without attack	-128.48200	159.96985	.708	-555.2598	298.2958
	HWMP without attack	812.44800*	159.96985	.001	385.6702	1239.2258
HWMP without attack	AODV without attack	-940.93000*	159.96985	.000	-1367.7078	-514.1522
	SAODV without attack	-812.44800*	159.96985	.001	-1239.2258	-385.6702

*. The mean difference is significant at the 0.05 level.

Post Hoc Tests are described in Table 5 discus the variation among each other. Thus energy consumption varies very less for the considered routing protocols under the varying condition of changing number of nodes. Table 6 discusses the descriptive like mean standard deviation for the three routing protocol under the effect of DDoS attacks.

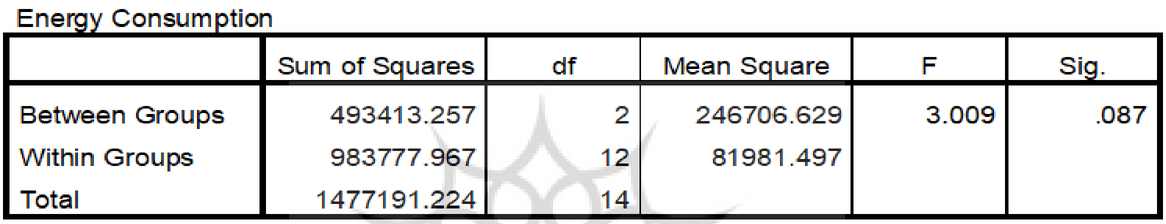
Table 6. Descriptive for three routing protocols in presence of attacks for energy consumption



Energy Consumption

		AODV with attack	SAODV with attack	HWMP with attack	Total	Model	
						Fixed Effects	Random Effects
N		5	5	5	15		
Mean		2708.7960	2416.2480	2272.9780	2466.0073		
Std. Deviation		277.07209	295.50266	286.10090	324.82866	286.32411	
Std. Error		123.91041	132.15281	127.94821	83.87040	73.92857	128.24628
95% Confidence Interval for Mean	Lower Bound	2364.7656	2049.3330	1917.7368	2286.1232	2304.9308	1914.2081
	Upper Bound	3052.8264	2783.1630	2628.2192	2645.8914	2627.0838	3017.8065
Minimum		2318.49	2011.35	1876.86	1876.86		
Maximum		3013.82	2765.86	2598.73	3013.82		
Between- Component Variance							32945.02627

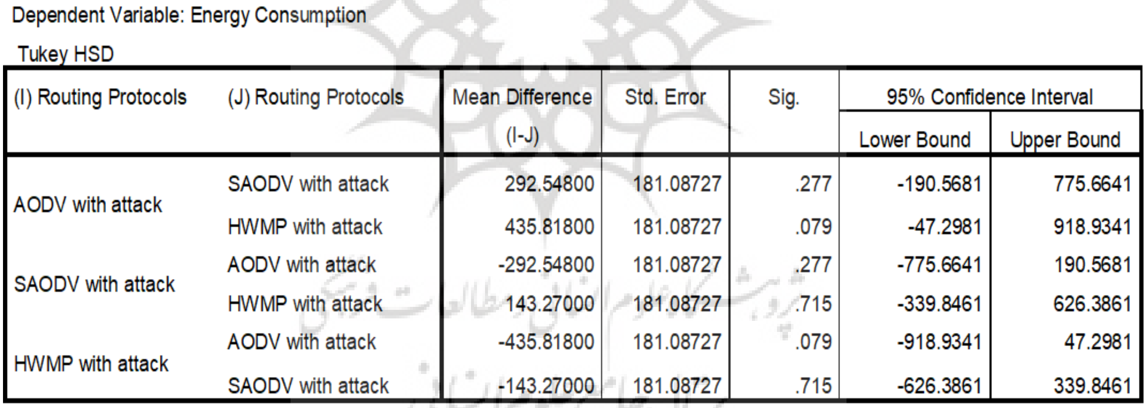
Table 7. ANOVA test for three routing protocols under influence of attacks



Energy Consumption

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	493413.257	2	246706.629	3.009	.087
Within Groups	983777.967	12	81981.497		
Total	1477191.224	14			

Table.8.Multiple Comparisons for three routing protocols in influence of attacks



Dependent Variable: Energy Consumption

Tukey HSD

(I) Routing Protocols	(J) Routing Protocols	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
AODV with attack	SAODV with attack	292.54800	181.08727	.277	-190.5681	775.6641
	HWMP with attack	435.81800	181.08727	.079	-47.2981	918.9341
SAODV with attack	AODV with attack	-292.54800	181.08727	.277	-775.6641	190.5681
	HWMP with attack	143.27000	181.08727	.715	-339.8461	626.3861
HWMP with attack	AODV with attack	-435.81800	181.08727	.079	-918.9341	47.2981
	SAODV with attack	-143.27000	181.08727	.715	-626.3861	339.8461

(Table 7) shown below discusses the ANOVA test for the three routing protocols under the influence of DDoS attacks. This includes the information about the SSB sum of squares between groups and sum of squares within groups along with degree of freedom. We reject the null hypothesis H_0. Post Hoc Tests represents the variation with respect to each other as shown in (Table 8).

The multiple comparisons for three routing protocols in the presence of attacks reflects that the mean variation in HWMP is less in comparison to the widely used reactive protocol AODV and secured protocol SAODV.

Conclusion

In this research study, the utilization of IOT-MANET based for handling the COVID -19 was emphasized in introductory section. Further to ensure optimized routing for the healthcare related data through smart phones the three routing protocols are considered and compared on the basis of average energy consumption. Thus for maintaining the privacy and patients security MANET based IoT devices could be used for handling patients to hospital management system and vice versa ; transmission of patient's complex data. This research study work scrutinized the performance of reactive (AODV, SAODV) protocols and hybrid HWMP, respectively, both in the absence and under the influence of DDoS attacks. Since monitoring the health conditions remotely is helping the healthcare professionals for tackling this novel coronavirus, thus the impact of DDoS attacks could lead to even death of patient. The simulation results of network simulator on the basis of one QoS parameter evaluates, HWMP overtakes from the two traditional routing protocols considered for different variation in speed for stable nodes number deliberated in the simulation. Under the influence of attacks for speed of 50 m/s for 30 fixed nodes, HWMP outperforms AODV and SAODV by 15.97% and 6.43% respectively for average energy consumption. The ANNOVA test, which is used one independent variable and dependent variable helps to study the correctness of result by looking at the table for both the scenario of in absence and presence of attacks. The mean plot describes that HWMP energy consumption is very less in contrast to reactive and secured protocol considered in study.

Future Work

In future the more QoS parameters like packet delivery ratio, Packet loss ratio, jitter, throughput and normalized routing load will also be compared among the three considered protocols in the investigation conducted, with different scenarios .The implementation of block chain can be worked upon in the interest of providing security majorly to the MANETS used in wireless mesh networks and in IoT MNAET based formed networks. Since the lots of emphasis has been on providing the privacy to the networks one the devices start connecting among each other via internet.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Agrawal, V. (2014, October). Security and privacy issues in wireless sensor networks for healthcare. In *International Internet of Things Summit* (pp. 223-228). Springer, Cham.

Alameri, I. A., & Komarkova, J. (2020, June). A Multi-Parameter Comparative Study of MANET Routing Protocols. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks." IEEE Access 7 (2019): 58221-58240.

Alharbi, T., Aljuhani, A., & Liu, H. (2018). SYN Flooding Detection and Mitigation using NFV. *International Journal of Computer Engineering and Information Technology*, *10*(1), 11-19.

Brill, C., & Nash, T. (2017, December). A comparative analysis of MANET routing protocols through simulation. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 244-247). IEEE.

Cai, C., Fu, J., Qiu, H., & Lu, Y. (2020, October). An Active Idle Timeslot Transfer TDMA for Flying Ad-Hoc Networks. In *2020 IEEE 20th International Conference on Communication Technology (ICCT)* (pp. 746-751). IEEE.

Chelli, K. (2015, July). Security issues in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the World Congress on Engineering* (Vol. 1, No. 20).

Cogliati, D., Falchetto, M., Pau, D., Roveri, M., & Viscardi, G. (2018, September). Intelligent cyber-physical systems for industry 4.0. In *2018 First International Conference on Artificial Intelligence for Industries (AI4I)* (pp. 19-22). IEEE.

Gautam, A., Mahajan, R. and Zafar,S.(2019).Implementing Blockchain Security to Prevent DDoS Attacks in Networks", *International Journal of Security and Its Applications (IJSIA),* Vol 13, No.4, pp 27-40.

Gautam, A., Mahajan, R., & Zafar, S. (2020). QoS Optimization in Internet of Medical Things for Sustainable Management. In *Cognitive Internet of Medical Things for Smart Healthcare* (pp. 163-179). Springer, Cham.

Gautam,A.,Mahajan, R., & Zafar, S. (2021). DDoS Attacks Impact on Data Transfer in IOT-MANET-Based E-Healthcare for Tackling COVID-19. In *Data Analytics and Management* (pp. 301-309). Springer, Singapore.

Singh,G and Singh,K.(2019).Detection and Prevention of Vulnerabilities in Open Source Software: An experimental study. *Journal of Discrete Mathematical Sciences and Cryptography, Taylor & Francis,* Vol 22, No 8**.**

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE access*, *3*, 678-708.

Jain, A. K., & Tokekar, V. (2015, January). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In *2015 International Conference on Pervasive Computing (ICPC)* (pp. 1-6). IEEE.

Khalaf, O. I., & Abdulsahib, G. M. (2020). Energy Efficient Routing and Reliable Data Transmission Protocol in WSN. *Int. J. Advance Soft Compu. Appl*, *12*(3).

Kumari,D., Singh,K. and Manjul,M.(2020).Performance Evaluation of Sybil Attack in Cyber Physical

System.In Proceedia of Computer Science Elsevier, India Volume 167, (pp 1013-1027).

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002, November). A secure routing protocol for ad hoc networks. In *10th IEEE International Conference on Network Protocols, 2002. Proceedings.* (pp. 78-87). IEEE.

Sharma, A. K., & Trivedi, M. C. (2016, February). Performance comparison of AODV, ZRP and AODVDR routing protocols in MANET. In *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)* (pp. 231-236). IEEE.

Siwach, V., Sehrawat, H., & Singh, Y. (2020). Energy-Efficient Schemes in Underwater Wireless Sensor Network: A Review. *Computational Methods and Data Engineering*, 495-510.

Walikar, G. A., & Biradar, R. C. (2017). A survey on hybrid routing mechanisms in mobile ad hoc networks. *Journal of Network and Computer Applications*, *77*, 48-63.

Yadav, P., & Agrawal, R. (2018). A Multi-homing Based Framework Against Denial of Service Open Threat Signaling in Healthcare Environment. *International Journal of Control and Automation*, *11*(11), 1-18.

Bibliographic information of this paper for citing:

Gautam, Ashu, Mahajan,Rashima & Zafar,Sherin, (2022). Energy Consumption Analysis of IoT-MANET based Systems with ANOVA Assessment for Tackling COVID-19. *Journal of Information Technology Management*, Special Issue, 89-102.