JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Evaluation and Management of Erroneous Data Transmission in MANETs with Non Repudiation of Hosts with Adhoc and Multipath Routing Protocols

[1]B.BARANI SUNDARAM, [2]Venkatesh andavar, [3]P.Karthika

[1]Associate Professor, [2]Assocoate Professor, [3]Professor
[1]Department of Computer and Information Technology,
[1]Defence University Engineering College, Bishoftu, Ethiopia

Abstract: To fulfill the fault tolerance requirements of MANETs, data link and network layer protocols must be created. In addition, when it comes to security, the most important issue is authentication. Because MANENTs work in a hostile environment, deploying PKI with a single certificate authority creates a single point of failure, forcing adversaries to look for a means to compromise the CA. As a result, the employment of distributed CAs appears to be obvious. The dispersed CA's provide a difficulty of service availability as MANETs expand in size. The distributed PKI must thus be localized to make it more available and safe.

The study described in this paper evaluated both the routing protocols that best suit fault tolerance and the appropriate authentication strategy, and made a detailed assessment of the candidate protocols and authentication schemes as a result. Multipath protocols are better in terms of fault tolerance, according to the study, and AOMDV and MDART were chosen as alternative fit in the framework based on network size.

IndexTerms **- AOMDV, ECDSA, Fault tolerance, MANETS, MDART, Security.**

I. Introduction

1.1Background

A Mobile Ad hoc Network (MANET) is a network of wireless mobile nodes that self-organize in arbitrary and transitory topologies. As a result, people and automobiles can be combined.

Internetworked in places where there is no pre-existing communication infrastructure or when using such infrastructure necessitates wireless expansion [1]. Mobile nodes in a mobile ad hoc network can communicate directly with all other nodes within their radio ranges, however nodes that are not in the direct communication range interact with each other through an intermediate node. In a network, communication entails sending data in the form of packets via particular ideal channels. The essential role of network communications is to find the best path (routing) for data transmission. Routing is done through routing algorithms that use metrics to determine which path is the best for a packet to take. A metric is a unit of measurement that includes things like path bandwidth and hop count. Routing algorithms set up and preserve routing information to make path decision possible.

The following are the various types of faults or mistakes that can arise in MANETs [2]:

Packet loss due to congested nodes/links, transmission faults, node failures, link failures, route breakages Because of malfunctioning network nodes or route failures, the performance of ad hoc routing protocols will suffer dramatically. Node mobility is the primary cause of route failures. Link failures due to wireless channel contention are another condition that might cause route failures. A route is made up of a series of links.

1.2 Definition of the issue

There is no central management or infrastructure support in MANETs. It is a target for attacks. Any node in the network can join and leave. As a result, security methods are critical in an ad hoc network. Unless some type of authentication mechanism is implemented into the network, node authentication is not assured by default. As a result, establishing node authentication and preserving the MANET fault-tolerant becomes a fundamental concern in MANET deployment.

1.3 The goal

The goal of this study is to assure maximum authentication strength across MANET nodes while preserving fault-tolerant data connection. The following are the precise goals of this thesis:

To use AOMDV and ECDSA to simulate fault-tolerant communication with malicious nodes.

To use MDART and ECDSA to simulate fault-tolerant communication with malicious nodes.

To compare AOMDV with MDART in terms of fault tolerance when using ECDSA.

To recommend the best alternative for MANET fault tolerance and security.

II. REVIEW OF THE LITERATURE

Following the literature analysis, we developed our proposed "Fault tolerant data transfer in mobile ad hoc networks without compromising the authenticity of nodes."

Analysis and selection of candidate schemes

Testing and recommending techniques that meet fault tolerance and authentication requirements in various contexts.

We divided our challenge into two layers based on our research: the routing layer and the security layer. We analyzed and selected candidates who fit into our layers based on the results of our poll. Finally, to back up our theoretical decisions, we conducted practical tests to further illustrate and improve our selections. Protocol simulations are run on a Linux operating system, Ubuntu 10.04, with ns-2.35. Throughout our simulation, we have performed various runs. Every simulation lasts between 0 and 200 seconds. In a rectangular field of 200m*200m, random waypoint mobility is used. At the time of execution, the TCL script imports traffic and mobility files.

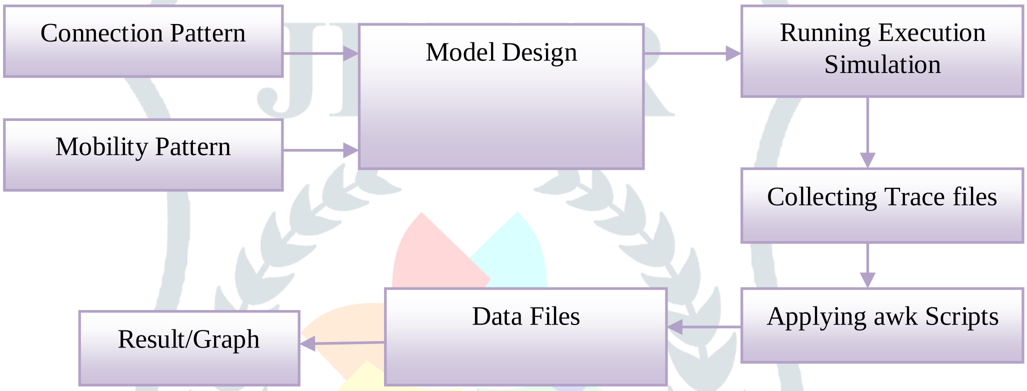

Figure 1: Simulation Process

III. MATERIALS AND TECHNIQUES

In order to evaluate the simulation environment and performance parameters, we used Network Simulator (version 2), often known as NS2.

NS2 outputs either text-based or animation-based simulation results after simulation. Tools like NAM (Network AniMator) and XGraph are used to evaluate these data graphically and interactively. The simulations are visualized using the network animator (nam).

AOMDV and MDART maintain a packet send buffer. The transmit buffer holds all of the data packets waiting for a route. The maximum size of an interface queue is 50 packets. All routing packets are held in IFQ until they are transmitted by the MAC layer. In general, the steps of simulation are depicted in the diagram below.

To carry out the simulation process of the above-mentioned protocols, follow the procedures below. Step 1: Scenarios are created using the above-mentioned setdest program, which employs a random waypoint mobility model. In this simulation, ten situations with varied maximum speeds are generated. The following is an example of a scenario generator: Setdest –n 50 – p 2 – M 20 –t 200 –x 200 –y 200 > scene50-01.sc Where -v stands for version 1 or 2, -n: the total number of nodes, -x and -y: simulation area, -t: simulation time, scene-50-01: output file

Step 2 - The cbrgen.tcl file from the indep utilities is used to build the traffic pattern. Only one traffic pattern is generated in this simulation using the following method:

cbr-50-40.sc> ns cbrgen.tcl - type cbr -nn 50 - seed 1.0 - mc 40 - rate 0.25>

Where - type: cbr or tcp traffic type - nn: the total number of nodes, - seed: value of the seed maximum connection sources (-mc) -rate: packet transmitting rate.

Step 3 - A tcl script is built to generate trace files after the traffic patterns and scenarios have been generated. These traffic patterns and scenarios are then supplied into the tcl script, which is then run. Trace files are created when a tcl script is run. Two protocols, AOMDV and MDART, are utilized in this simulation to generate trace files with the extension *.tr, which are archaic trace file formats. There are two types of trace file formats: old trace file format and new trace file format. A *.nam file is created along with the trace file, which illustrates the animation of the moving nodes and packet routing. *.nam files are useful for displaying packet routing and node mobility.

Step 4 – Once trace files have been generated, they must be analyzed using awk or a script. Awk scripts are built to examine the files based on the performance metrics that will be utilized in the performance review. This simulation is used to assess performance using three metrics: packet delivery fraction, average end-to-end delay, and throughput.

Step 5 – After analyzing the trace files, the results are saved in a text file and shown as graphs using Microsoft Office Excel, Math Lab, or the ns-2 X graph software. The studied results are saved in a text file, and graphs are displayed using Microsoft Office 2007 Excel between both models and performance measures such as packet delivery fraction, average end to end delay, and throughput.

IV. Metrics of Performance

Table 1: Simulation Parameters for Number Nodes Model

Parameters	Values	
Routing Protocol	AOMDV	MDART
Number of Nodes	50,55,60,65,70,75,80	50,55,60,65,70,75,80
Simulation Time	200	200
Environmental Size	200 * 200	200 * 200
Traffic Type	CBR(constant bit rate)	CBR(constant bit rate)
Packet Size	512 byte	512 byte
Packet Rate	0.25	0.25
Maximum Speed	20	20
Queue Length	50	50
Mobility Model	Random Waypoint	Random Waypoint
Antenna Type	Omni-Directional	Omni-Directional

Table 2: Simulation Parameter for Malicious Node Model

Parameters	Values	
Routing Protocol	AOMDV	MDART
Number Malicious of nodes	0,1,2,3,4,5,6,7,8,9,10,11	0,1,2,3,4,5,6,7,8,9,10,11
Simulation Time	200	200
Number of node	50	50
Pause Time	2	2
Environment Size	200 * 200	200*200
Traffic Type	CBR(constant Bit Rate)	CBR(constant Bit Rate)
Packet size without security, packet size with security	512 Byte, 832 Byte respectively	512 Byte, 832 Byte respectively
Packet Rate	0.25	0.25
Maximum Speed	20	20
Maximum connection	40	40
Queue Length	50	50
Mobility Model	Random Waypoint	Random Waypoint
Antenna Type	Omni-Directional	Omni-Direction

Table 3: Simulation Parameters for Pause Time Model

Parameters	Values	
Routing Protocols	AOMDV	MDART
Number of nodes	50	50
Simulation Time	200	200
Pause time	5,10,15,20,25,30	5,10,15,20,25,30
Environmental size	200 * 200	200 * 200
Traffic Type	CBR(constant bit rate)	CBR(constant bit rate)
Packet size	512	512
Maximum speed	20	20
Maximum connection	40	40
Queue Length	50	50
Mobility Model	Random Waypoint	Random Waypoint
Antenna type	Omni-Directional	Omni-Directional

The ratio of data packets delivered to the destination to those generated by the sources is known as the packet delivery fraction. It's determined by multiplying the number of packets received by destination by the number of packets sent from the source. PDF = total packets received / total packets sent

Average end-to-end delay - This covers all possible delays caused by buffering during route discovery latency, interface queue queuing, MAC retransmission delay, propagation, and transfer time. It is the time it takes for a data packet to travel from source to destination through a MANET.

D = (Receive time – Sent time) / total number of received data packets

Average Throughput is the number of packets successfully delivered to each individual destination divided by the overall duration.

Models and simulation parameters are being tested.

For simulation, three main types of models are employed, as shown below.

Changing the number of malicious nodes while keeping the number of nodes, stop duration, transmission rate, number of flows, and node speed constant.

Node model - variable node number, but constant pause duration, transmission rate, number of flows, and node speed.

Model with variable stop time but fixed number of nodes, transmission rate, number of flows, and node speed.

The table below lists the simulation parameters utilized for these three models.

Table 4: Without the Presence Security

No. of Malicious Nodes	Throughput		PDF		Average end-to-end Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
0	24.14	23.92	0.9992	0.9940	0.006340	0.006798
1	24.14	22.90	0.9992	0.9630	0.006340	0.006887
2	22.17	20.06	0.9224	0.8491	0.006366	0.006864
3	20.48	18.00	0.8606	0.7539	0.006411	0.006971
4	19.85	17.35	0.8325	0.7277	0.006383	0.007247
5	18.78	14.50	0.7715	0.6159	0.006463	0.007023
6	17.72	14.06	0.7306	0.5804	0.006456	0.006720
7	16.29	12.17	0.6743	0.5060	0.006528	0.006744
8	15.57	11.72	0.6474	0.4901	0.006553	0.006701
9	14.37	9.18	0.5951	0.3800	0.006604	0.006689
10	13.53	8.57	0.5631	0.3561	0.006603	0.006695
11	12.62	6.91	0.5172	0.2873	0.006632	0.006649

Table 5: With the Presence of Security

No. Malicious Nodes	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
0	23.97	23.55	1.0000	0.9957	0.009271	0.009781
1	23.97	23.11	1.0000	0.9616	0.009271	0.009493
2	22.39	20.68	0.9216	0.8536	0.009158	0.009671
3	20.55	18.11	0.8580	0.7543	0.009212	0.009446
4	20.06	17.54	0.8360	0.7279	0.009258	0.009639
5	18.76	14.60	0.7736	0.6085	0.009381	0.009425
6	17.23	13.78	0.7351	0.5798	0.009256	0.009525
7	16.33	12.13	0.6783	0.4987	0.009334	0.009324
8	15.80	11.43	0.6595	0.4840	0.009353	0.009349
9	14.38	9.32	0.6031	0.3812	0.009431	0.009368
10	13.84	8.48	0.5746	0.3542	0.009423	0.009380
11	12.40	6.92	0.5167	0.2852	0.009568	0.009360

Table 6: Varying Pause Time

Pause Time	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
5	23.94	23.25	1.0000	0.9947	0.006375	0.007047
10	24.24	23.53	1.0000	0.9939	0.006367	0.006891
15	23.94	24.05	1.0000	0.9966	0.006244	0. 006812
20	24.17	23.51	1.0000	0.9931	0.006390	0. 006835
25	24.42	24.06	1.0000	0.9966	0.006405	0.006899
30	23.85	23.97	1.0000	0.9966	0.006380	0.007170

Table 7: Varying Size Network

No. of Nodes	Throughput		PDF		Average End-to-End Delay	
	AOMDV	MDART	AOMDV	MDART	AOMDV	MDART
50	23.77	24.01	1.0000	0.9974	0.006410	0.006966
55	23.88	23.82	1.0000	0.9949	0.006057	0.006996
60	24.28	23.86	1.0000	0.9932	0.006392	0.007631
65	24.03	23.88	1.0000	0.9940	0.006089	0.007971
70	24.01	24.03	1.0000	0.9949	0.006408	0.008711
75	23.98	23.64	1.0000	0.9923	0.006097	0.012892
80	23.92	23.47	1.0000	0.9896	0.006422	0.034144

IV. RESULTS AND DISCUSSION

We also looked at how the addition of security affected the performance of both protocols. Furthermore, based on our findings, we calculated the impact (fault tolerance) of introducing a certain number of rogue nodes into a network. As a result, we've compiled a summary of our findings below.

REFERENCES

[1] A.Nedumaran, R.Ganesh Babu, Mesmer Mesele Kass, and P.Karthika, 2019. Machine Level Classification Using Support Vector Machine. AIP Conference Proceedings of International Conference on Sustainable Manufacturing, Materials and Technologies (ICSMMT 2019), Coimbatore, Tamil Nadu, India, pp. 020013-1–020013-10, October 25-26,.

[2] P. Karthika and P. Vidhya Saraswathi, 2017. A Survey of Content Based Video Copy Detection Using Big Data. Int. J. Sci. Res. Sci. Tech., vol. 3, pp. 114-118, March-April.

[3] Dr.B.Barani sundaram1, dr. Balachandra pattanaik, dr.n.kannaiya raja, mr.elangovan.b,dr. Kaja masthan, mr.balam suresh kumar, 2020. performance suitability interms of fault tolerane of manet's on aomdv and mdart in combination with ecds. journal of critical reviews, issn- 2394-5125 vol 7, issue 14.

[4] Dr.B.Barani Sundaram, Mr.Tucha Kedir Elemo, 2020. Node isolation attack on olsr ,reputation relied Mitigation. Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9), ISSN 1567-214x,.

[5] Dr.B.Barani Sundaram, Mr.Tucha Kedir, Mr.Tesfaye Tadele Sorsa, Mr. Rabira Geleta, Dr.Nune Srinivas, Adola Haile Genale, 2020. An Approach for Rushing Attack Resolution in Aomdv Using Arbitrary Id in Manet. Palarch's Journal of Archaeology of Egypt/Egyptology,.

[6] B.Barani Sundaram, N.Kannaiya Raja, Nune Sreenivas, Manish Kumar Mishra, Balachandra Pattanaik, , P.Karthika, 2020. RSA Algorithm using Performance Analysis of Steganography Techniques in Network Security. International Conference on Communication, Computing and Electronics Systems (ICCCES 2020) 21-22, October.

[7] B.Barani Sundaram, Mr.Tucha Kedir, Manish Kumar Mishra, Seid Hassen Yesuf, Shobhit Mani Tiwari, and P.Karthika,2021. Security Analysis for Sybil Attack in Sensor Network using Compare and Match-Position Verification Method. Second International Conference on Mobile Computing and Sustainable Informatics (ICMCSI 2021).

[8] Dr.B.Barani Sundaram , Dr.Amit Pandey, Mr.Aschalew Tirulo Abiko, Mr Janga Vijaykumar,Mr.Adola Haile Genale, P.Karthika,2021. Wireless Sensor Network to Connect Isolated Nodes using Link Assessment Technique," 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).

[9] Dr.B.Barani Sundaram, Mr.Tucha Kedir, Mr.Tesfaye Tadele Sorsa, Dr.Nune Sreenivas, Dr. Manish Kumar Mishra, Mr.Dhanapal Thirumoorthy, Karthika.P, 2020. STEGANALYSIS FOR IMAGES SECURITY CLASSIFICATION IN MACHINE LEARNING USING SVM. 4th International Conference on Computational Vision and Bio Inspired Computing (ICCVBIC 2020), .

[10] B.Barani Sundaram,Sudhanshu Maurya, P.Karthika, P. Dr.P.Vidhya Saraswathi,2021. Enhanced the Data Hiding in Geometrical image using stego-Crypto techniques with machine learning. 6th International Conference on Inventive Computation Technologies.

[11] Dr.B.Barani Sundaram, Dr P Rajkumar . Mrs M. Ananthi , Dr V Sravan Kumar ,Mr Janga Vijaykuma, P.Karthika, 2020. Network Security Analysis for Signal Strength Based Packet Filitering. 3rd International Conference on Intelligent Sustainable Systems.

[12] B.Barani Sundaram, Nune Srinivas, Tucha Kedir Elemo, Manish Kumar Mishra, Dhanabal Thirumoorthy and Tesfaye Tadele Sors,2020. Renewable Energy Sources Efficient Detection in Triangulation for Wireless Sensor Networks", International Virtual conference on Robotics. Automation, Intelligent Systems and Energy.

[13] Seelam Sowjanya,Barani Sundaram,2018. OVERVIEW ON E-VOTING SYSTEM AND SECURITY CHALLENGES," http://www.ijaerd.com/index.php.

[14] Seelam Sowjanya,Barani Sundaram, 2018. Discovering IP Spoofers Locations From Path Backscatter. http://ijsart.com/Home/IssueDetail?id=21325,

[15] Dr.B.Barani Sundaram, Miss.Seelam Sowjanya, Dr.Venkatesh Andavar, Dr.N.R.Reddy, 2018. Opportunities and Challenges of E-Commerce in the Case of Ethiopia. International Journal for Research in Technological Studies| Vol. 5, Issue 4, March 2018 | ISSN (online): 2348-1439,.

[16] Dr.B.Barani Sundaram, Seelam Sowjanya, Dr.Venkatesh Andavar, Dr.N.R.Reddy, 2018. Effectiveness of Geographic Information System and Remote Sensing Technology as a Decision Support Tool in Land Administration the Case of Yeka Sub City. Addis Ababa International Journal of Innovative Research in Science, Engineering and Technology Vol. 7, Issue 3, March 2018,ISSN(Online): 2319-8753,ISSN (Print): 2347-6710,.

[17] Seelam Sowjanya ,Dr.Barani Sundaram, 2018. REVIEW ON STYLIZATION ANALYSIS USING STYLOMETRIC APPROACH," International Journal for Science and Advance Research In Technology (INTERNATIONAL PEER REVIEWED OPEN ACCESS JOURNAL) ISSN [Online] : 2395-1052.

[18] Seelam Sowjanya, Dr.Barani Sundaram | Sisay Deresa," HUMANS EMOTIONS EXTRACTION FROM IMAGE ANALYSIS, 2018. International Journal for Science and Advance Research In Technology (INTERNATIONAL PEER REVIEWED OPEN ACCESS JOURNAL) ISSN [Online] : 2395-1052,.

[19] Dr. Kaja Masthan, Mr. Balam Suresh Kumar, Dr. B. Barani Sundaram, Dr. Balachandra Pattanaik, Mr. Elangovan B., Dr. N. Kannaiya Raja,2020. Approach for Active Event Correlation for Detecting Advanced Multi-Level Cyber-Attacks. Solid State Technology Vol. 63 No. 2s.

[20] B. Elangovan, Dr.N. Kannaiya Raja, Dr. Kaja Masthan, Balam Suresh Kumar, Dr.B. Barani Sundaram, Dr. Balachandra Pattanaik,2020. The Image Steganographic Method to Hide the Secret Text in an Image Using Spiral Pattern and Cryptographic Technique to Increase the Complexity for Eavesdropper. Journal of Adv Research in Dynamical & Control Systems, Vol. 12, 08-Special Issue.

[21] Barani Sundaram, B., Pandey, A., Abiko, A.T., ...Genale, A.H., Karthika, P,2022. Analysis of Machine Learning Data Security in the Internet of Things (IoT) Circumstance. Lecture Notes in Networks and Systems, 2022,209, pp. 227–236.

[22] Barani Sundaram, B., Kedir, T., Mishra, M.K., ...Tiwari, S.M., P. Karthika,2022. Security Analysis for Sybil Attack in Sensor Network Using Compare and Match- Position Verification Metho. Lecture Notes on Data Engineering and Communications Technologiesthis link is disabled, 68, pp. 55–64,.

[23] Thirumoorthy, D., Rastogi, U., Sundaram, B.B., ...Pattanaik, B., Karthika, P, 2021. An IoT implementation to ATM safety system," Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021, pp. 744–749.

[24] Andavara, V., Sundaram, B., Bacha, D., Dadi, T., Karthika, P.,2021. The Impact of Perceived Ease of Use on Intention to Use Mobile Payment Services for Data Security Applications. Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021, pp. 1875–1880.

[25] Pattanaik, B., Barani Sundaram, B., Mishra, M.K., Thirumoorthy, D., Rastogi,2021. Industrial Speed Control of im Based Model Predictive Controller Using Zeta Converter. Journal of Physics: Conference Series, 1964(6), 062075.

[26] Rastogi, U., Pattanaik, B., Barani Sundaram, B., Mishra, M.K., Thirumoorthy, D., 2021. Investigation of DSR protocol performance in Wireless MANET using Correlation Method. Journal of Physics: Conference Series, 1964(4), 042042.

[27] Barani Sundaram, B., Mishra, M.K., Thirumoorthy, D., Rastogi, U., Pattanaik, B., ZHLS,2021. Security Enhancement by integrating SHA256, AES, DH in MANETS. Journal of Physics: Conference Series, 1964(4), 042003,.

[28] Pattanaik, B., Hussain, S.M., Kumar, R.S., Sundaram, B.B.,2021. Design of Smart Inverter for Distribution system using PV-STATCOM. International Conference on Intelligent Technologies, CONIT 2021.

[29] Sundaram, B.B., Pandey, A., Abiko, A.T., ...Genale, A.H., Karthika, P.,2021. Wireless sensor network to connect isolated nodes using link assessment technique. Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV),Pages 39-42,Publisher IEEE.

[30]Assefa Senbato Genale, B.Barani Sundaram, Amit Pandey, Vijaykumar Janga, Desalegn Aweke,.P. Karthika,2022. Big Data Analysis for knowledge based on Machine Learning using Classification Algorithm. Date Added to IEEE Xplore: 27 April.

[31]Desalegn Aweke, Assefa Senbato Genale,B. Barani Sundara, Amit Pandey,Vijaykumar Janga,Karthika, P.,2022. Machine Learning based Network Security in Healthcare System. Date Added to IEEE Xplore: 27 April.

[32]B.Barani Sundaram, 2013. An Approach for Surface Modeling Through Quad Orthogonal Mesh Generation. Defence Engineering Journal Of Ethiopia.

[33]B.Barani Sundaram, 2013. Tetrahedral Mesh Generation with Controlled Directionality. Bulletin of Pure and Applied Sciences,volume 30 E,Issue(no2) 2013:P.287-302, www.Bpas.in

[34]B.Barani Sundaram,3 D triangle mesh generation ESEE -2013,Bahardhar University,Ethiopia

[35]B.Barani Sundaram, 2016. Performance Analysis of Routing protocols in MANET for Fault Tolerant Data Communication WURCSO. wollo university, May18,2016.Desse.

[36]B.Barani Sundaram, 2017. Performance evaluation of SSL v.3and ECC against RSA over network communication between Client and Server. 5th international Conference on AST,Bahirdhar University, ,Bahirdhar, Ethiopia.

[37]B.Barani Sundaram,Sudhanshu Maurya, P.Karthika, P. Dr.P.Vidhya Saraswathi, 2021. Enhanced the Data Hiding in Geometrical image using stego-Crypto techniques with machine learning. 6th International Conference on Inventive Computation Technologies.

[38]Dr.B.Barani Sundaram Dr P Rajkumar . Mrs M. Ananthi , Dr V Sravan Kumar ,Mr Janga Vijaykuma, P.Karthika, 2020. Network Security Analysis for Signal Strength Based Packet Filitering. 3rd International Conference on Intelligent Sustainable Systems (ICISS 2020).

[39]B.Barani Sundaram, Nune Srinivas, Tucha Kedir Elemo, Manish Kumar Mishra, Dhanabal Thirumoorthy and Tesfaye Tadele Sors, 2020. Renewable Energy Sources Efficient Detection in Triangulation for Wireless Sensor Networks. International Virtual conference on Robotics, Automation, Intelligent Systems and Energy (IVC-RAISE 2020).

[40]Seelam Sowjanya,Barani Sundaram,2018. OVERVIEW ON E-VOTING SYSTEM AND SECURITY CHALLENGES. http://www.ijaerd.com/index.php.

[41]Seelam Sowjanya,Barani Sundaram,2018. Discovering IP Spoofers Locations From Path Backscatter. http://ijsart.com/Home/IssueDetail?id=21325

[42]Dr.B.Barani Sundaram1 Miss.Seelam Sowjanya2 Dr.Venkatesh Andavar, Dr.N.R.Reddy, 2018. Opportunities and Challenges of E-Commerce in the Case of Ethiopia International Journal for Research in Technological Studies| Vol. 5, Issue 4, March 2018 | ISSN (online): 2348-1439

[43]Dr.B.Barani Sundaram, Seelam Sowjanya, Dr.Venkatesh Andavar, Dr.N.R.Reddy 2018. Effectiveness of Geographic Information System and Remote Sensing Technology as a Decision Support Tool in Land Administration the Case of Yeka Sub City. Addis Ababa International Journal of Innovative Research in Science, Engineering and Technology Vol. 7, Issue 3, March 2018,ISSN(Online): 2319-8753 ISSN (Print): 2347-6710.

[44]Seelam Sowjanya ,Dr.Barani Sundaram, 2018. REVIEW ON STYLIZATION ANALYSIS USING STYLOMETRIC APPROACH. International Journal for Science and Advance Research In Technology (INTERNATIONAL PEER REVIEWED OPEN ACCESS JOURNAL) ISSN [Online] : 2395-1052.

[45]Seelam Sowjanya | Dr.Barani Sundaram | Sisay Deresa, 2018. HUMANS EMOTIONS EXTRACTION FROM IMAGE ANALYSIS. International Journal for Science and Advance Research In Technology (INTERNATIONAL PEER REVIEWED OPEN ACCESS JOURNAL) ISSN [Online] : 2395-1052.