A Framework Enduring Authentication and Collision Avoidance in AODV Routing Protocol

[1]Kollu Spurthi, Research Scholar,

[#2]T.N.SHANKAR, Professor,

Dept of CSE, Koneru Lakshmaiah Education Foundation, Vaddesvaram, Guntur,AP,India.

Abstract

MANETs proved to be the top choice of Researchers, as networks owe to be the spine of communications. The efficiency of Ad hoc environments relies on the design of well-versed routing protocols for the transfer of data between nodes. Several such protocols occupied the workspace, focusing on advancements in a performance environment with broad categorization into Proactive, Reactive, and Hybrid. Speculating on their nature of routing information several variations like DSDV, OLSR, DSR, AODV, and ZRP captivate the practitioner's domain. Source initiated on-demand protocols rank higher in outcome in contrast to Table driven, motivating our work to emphasize on AODV protocol belonging to the former category. AODV protocol with all strong features combats against degrading parameters like collisions, energy consumption, and security hurdles. These performance evaluating factors of Research gaps are better handled in our proposed approach by embedding Geographic Adaptive Fidelity algorithm with AODV resulting in lowered energy loss at nodes and with hands-on privacy retention using homomorphic encryption. This advanced combined technique E-AODV, simulated on NS3.2 yields outstanding results in terms of throughput, Delay, Load balancing, and delivery ratio.

Key words: *AODV, GAF, Homomorphic Encryption, Attacks, Routing protocols;*

1. Introduction

Widespread adoption of wireless networks since the 1990s made MANETs a popular research area with several academic enhancements. It is a decentralized wireless network with ad hoc characteristics of dynamically transforming infrastructure. Manet's do not rely on predefined topologies instead every node involves forwarding data to other nodes depending on the connectivity of nods and routing protocols. These accepted features of ad hoc networks expose their applicability in a decentralized environment with wide scalability. Ease of deployment of ad hoc networks makes it an apt choice even for emergency options like disaster and military issues.

Various Ad hoc networks can be classified concerning their usage as MANET's, VANET's, SPANS, iMANET's, Army tactical manet's,Airforce UAV networks, Wireless sensor networks, Data monitoring and mining, Disaster management ad hoc networks, Ad hoc for robots, streetlights, smart lighting and many more. The availability of adaptive and dynamic routing protocols supports the formation of ad hoc networks at a faster rate.

Routing protocols, the backbone for Ad hoc networks generally occupy one of the three categories like Proactive, Reactive, and Hybrid. Proactive differs from other protocols with a fact that it maintains updated routing information through interval-based exchanges [19]. They work well with a backlog that they react slowly to failures and require more data for maintenance. Contemporary Reactive protocols vote in identifying the best route for packet delivery with user and traffic demand requirements. It uses Route request packets to identify the intended route for the packet. Our protocol of interest falls into this category. Finally, the Hybrid protocol leverage the benefits by combining the advantages of both proactive and reactive, ie routing initiated with proactive information and later extends the service to newly activated nodes on-demand with reactive flooding property.

These routing protocols in some way are subjected to adverse effects resulting in detonating the overall network performance. Few parameters involved in these aspects are energy consumed, collisions, andsecurity vulnerabilities like wormhole attack[17], black hole attack, grey hole attack [8], and so on which reduce the network functionalities by shortest path illusions and malicious nodes [13] that are discussed in our experimental consideration. Few attacks can be handled with ease using legacy encryption and steganographic techniques by data encapsulation [25].

As nodes participating in routing have restrictions on battery life, energy consumption becomes a dictating factor to be regulated. This factor can be tuned by introducing pre-existing algorithms like GAF, SPAN, Topology management by priority ordering (TMPO), Adaptive neighbors based topology control (ANTC)[15]. The GAF helps in drilling down the energy consumed with spurious nodes deactivation and maintaining static fidelity levels in the network. GAF Algorithm is not affected by underlying

Manuscript received November 5, 2020
Manuscript revised November 20, 2020
https://doi.org/10.22937/IJCSNS.2020.20.11.15

protocols extending the scope for implementation in combination with pre-existing Routing protocols[7]. Span works by selecting a few nodes as co-ordinators for performing multi hop routing [5], meanwhile, other nodes sleep in power saving mode to conserve energy. TMPO works using MDB (Minimal Dominating set) and CDS (Connected Dominating Set) generated with 2 hops neighborhood information. ANTC on other hand defines transmission range adaptively for securing connectivity. Depending on in-range connectivity each node opts for a backbone that promises a hierarchical network [27].

Collisions, an interesting factor deciding the MANET efficiency are caused due to overwhelming beacon packets, evolving topologies and dynamically moving nodes resulting in packet loss[20]. This is an unaccepted issue in terms of reliable data transmission. So, such collisions need to be avoided and remedies are proposed by several researchers.

Ad hoc networks, attack prone [1] with their dynamic characteristic nature leading to loss of security services like authentication, confidentiality [26], integrity, and reliability. Several attacks compromise these security services and open into network causing undesirable consequences. Our proposed model emphasizes the above-discussed issues and defines an enhanced methodology to wrap up these gaps by combining GAF with AODV routing and thereby reducing security threats considering homomorphic encryption with a mobile sink. This combination deliberately projects an increased curve in the overall performance concerning QoS parameters of networks.

2. Related Works

Gupta. A, and Rana .K (2015) reviewed various for detection and prevention of Blackhole and gray hole attacks in AODV. Keshavarz, H., Noor, R. M., & Mostajeran, E. (2013) proposed a routing table flag for verifying the status and determining the node condition in AODV.Grover, J., Shikha, & Sharma, M. (2014) discussed in detail about GAF and introduced a methodology to decrease the energy used by nodes in the route establishment phase. Mittal, S., Kaur, R., & Purohit, K. C. (2016) talked about AODV in a detailedand proposed AODV-AP technique that initiates a new route when established route link breaks. Mafirabadza, C., & Khatri, P. (2017) worked to propose energy-efficient AODV, whose performance when compared to the existing system. Deepak.S, & Anand.H (2019) talked in detail about RREQ, RREP, RERR packets, their functioning, route establishment, route maintenance in the AODV routing protocol.Parmar, M. K., & Jethva, H. B. (2014)analyzed the effect of a black hole, gray hole attack in AODV using simulation. Xu, Y., Heidemann, J., & Estrin, D. (2001) introduced GAF that conserves energy by switching off spurious nodes in routing and simulated GAF over AODV and DSR.Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. (2001) talked about SPAN, an energy conservation algorithm that saves power using the co-ordinator node.Belghith, A., Belhassen, M., Dhraief, A., Dougui, N. E., & Mathkour, H. (2015)presented CE-OLSR optimized routing protocol to reduce the impact of obstacles with zero signal overhead and analyzed the proposed technique using OMNET ++. Srinivas, Murthy, Sainath P, and Vishnu J (2019) came forward with detailed content-centric MANETS (CCMANETS) and introduced efficient multicasting and collision avoidance (EMCA) protocol to avoid collisions and packet loss. Rajan. P and Kamboj .P proposed a key distribution mechanism using stenography for link encryption in AODV to enhance security.Awadhesh Kumar and R. R. Tewari (2017) suggested an asymmetric key technique in AODV for secure route discovery and route reply messages. Amir and Chris (2005) contributed a secure AODV protocol to thwart the security hurdles in wireless networks.Anguraj, D. K., & Smys, S. (2018) handled malignant nodes using varied trusts like energy, data, and communication by proposing Trust based IDS.Ziwei, Y., Amrit, M., Lixia, Y., Sidheswar, R., & G, P. (2018) contributed vector optimization to identify the active nodes with mathematical computations.Spurthi. K, Srinivasarao Tammireddy, Satyabrata Patro, T. N. Shankar, G. Swain, and Ranjan K. Senapati (2016) proposed IDS based EAACK technique for identifying malicious nodes in AODV Routing protocol. Spurthi. K and NarayanShankar T.,(2017), reviewed several routing protocols in detail for the possible attacks in Wireless networks. Spurthi. K and T N Shankar (2020) came up with k-means based LGF to overcome several attacks like a wormhole and black hole. Roychowdhury and Petra (2010) proposed an Energy-aware GAF for Geographical routing in ad hoc networks. Sun, X., Yu, F. R., Zhang, P., Xie, W., & Peng, X. (2020) discussed in detail homomorphic encryption for secure computation based on ciphertext avoiding decryption. Ray, N. K., & Turuk, A. K. (2016) proposed location-based topology control including sleeping schedule in Ad hoc networks with topology and power management schemes. Liu, S., Yang, Y.,& Wang, W. (2013) discussed Route Establishment, maintenance with RREQ, and RREP packets in the AODV routing protocol. Xinlian, Z., & Zepeng, Z. (2017) proposed a new GAF algorithm using a cluster head and sink node with node residual energy concept embedded. Pradhan, A., Raja Sekhar, K., Swain (2017) discussed about steganography with LSB to hide data bits. Sekhar, LSS Reddy, UJ Kameswari, (2012) analysed about different security attacks and how firms can handle them. Krovi Raja Sekhar, Veerapaneni, S.S., (2020) Proposed model for organizational security from breaches.

3. Basic Preliminaries

AODV: An Ad hoc on-demand distance vector routing protocol is one among the few protocols of concern preferred for studies by Researchers and Practitioners. This protocol by definition is initiated by the source with an RREQ packet routed towards the recipient with an address match criterion [2] [18]. The intended destination node acknowledges back with an RREP [6] to source initiated communication by establishing a route. AODV also entails a few short comings like [10,12].

a) Congestion and collisions raising from the common shortest path result in heavy packet loss [4].
b) Node strenuous action during route identification prompts the breakage of route reflecting in RREP packet loss [9].
c) Overhearing by nodes in the network results in higher energy consumption with unwanted nodes participating in the conversation and consuming energy[11].
d) Security aspects like confidentiality integrity and authentication are at risk due to malicious nodes in the network. Symmetric key-based approaches are unsuccessfulin handling the issue [3].

GAF: Energy consumption in wireless networks imposes a strong challenge in the overall network performance of nodes in Ad hoc networks that perform information gathering from other nodes consuming large amounts of energy [16]. Energy conservation mainly deals with power management and controlled topology. Power management is entertained by 3 states active- consumes power, ideal-just halts in wait mode, and sleep- turns off the transmitter and receiver [15]. A well-versedsolution to handle this problem is by adopting the GAF algorithm. It makes use of node information, direction, and neighbors to build the desired topology. Location information is inherited by using a global positioning system that sounds expensive[22]. The direction depends on the angle of arrival methodology and topology depends on neighborhood information. In our approach, GAF reduces the energy absorbed by turning off the undesired nodes whose participation does not mandate the transmission[23,24].

Homomorphic Encryption: Encryption of data aims at rendering data security from Intruders during transmission in the networks. Various encryption techniques served the security requirements among which homomorphic encryption is considered for present work. It allows numerable types of operations to be carried out on coded data without disclosing the secret key[21]. The transferred data maps the decrypted computation. This encryption algorithm proceeds in the following stepwise manner, for security purposes, consider HME as the Encryption scheme. It considers 4 parameters Genkeys, E_k, D_k, valuating-fun.

1) HME_Genkeys (1^{λ}): The input λ is the security parameter and leads to output values public key key_pub, a secret key -key_sec, and key evaluation K_{evk}.
2) HME E_k : The key_pub and plaintext P are inputs with output ciphertext C_P i.e.
   C_P= HME _E_K (key_pub, P).
3) HME _D_K: The secret key key_sec and cipher C_P are inputs with P defined as
   P = HME_D_K (key_sec, P).
4) HME _Valuating_fun : Inputs are evaluation function key K_{evk} , function f_1 and ciphertext C_0....C_{m-1} , where plaintext for C_i is P_i , i=0....m-1 and function is computed as
   C_{f1}=HME_Valuating_fun(K_{evk},f1,C_0....C_{m-1})

4. Proposed Approach

The Proposed approach presents a model that explicitly renders performance efficiency in the comparison between the notions of expected and available impact level of satisfaction in evaluation issues among prior and post scenarios. Thegoal of the proposed model is to emphasize the possible limitation in the existing system and follow with a profound solution to roll up to adverse effects. Our model employs the AODV routing protocol with GAF and increments with homomorphic encryption. The Model flows in the following phases.

Few assumptions are taken into consideration like the network is divided into regions, every region is headed by a mobile sink responsible for path establishment, Transmission, and security.

1) The phase starts with the source initiating the route discovery packet by forwarding the RREQ packets to the deployed mobile sink.
2) The mobile sink plays a vital role in route establishment by generating the secured keys for path establishment with a homomorphic encryption scheme. It keeps track of all node information within the defined region and thereby provides an alternate path for different nodes to overcome collisions that leads to packet loss.

3) The secure route established by mobile sink works in conjunction with GAF to reduce energy consumption by initiating a sleep state in nodes that do not participate in transmission.
4) The path generated by the mobile sink is considered by the source node to initiate data transfer to the indented destination node.
5) The communication ends successfully with the key provided by the mobile sink without collisions and security-enhanced.
6) The mobile sink ensures a collision-free path by allocating a unique route between nodes to initiate communication.

Algorithm for the Proposed Model :

// Encrypted node selection process
1: Divide the plaintext into 88-bitsNblocksS=fb1;b2;...;bN. At each node
2: Build the 176-bits bit sequence b
3: Separate b to two equal parts p1and p2, 88-bits each
4: Compute the count of 1's for each byte X[x1;x2;...;x8] as well as count of 1's for each 11 bits Y[y1;y2;...;y8] inp2
5:fori=1;2;...;N do
6:d=p1bi
7:d=Perm {d; X[i] }, where Perm is the permutation function.
8:a=Con {d; Y[i] }, where Con is the concatenation function.
9:Cipher[i] =a
10:end for
11: Return the ciphertext Cipher [c1;c2;c3;...;cN] , where ci is the ciphertext of b

//Decrypted node selection process with secure communication
1: consider ciphertext C with size b bits from CH x, get the count of its cluster members N.
2:g= the first(N*176)bits of C, where g is the aggregated data.
3:l=C-g, where l is the cluster members' IDs starting from bit index(N*176)þ1ofC
4:g= Deaggr(g), where Deaggr is the de-aggregation function that reverses the homomorphic operation
5:Ci=Assign {g;l}, where Ci is the ciphertext of SNi
6:fori=1;2;...;N do
7: Partition Ci into 88-bitsQsegmentsS=fs1;s2;...;s Ng
8: Generate the 176-bits bit sequence b
9: Divide b into two equal partsp1andp2, 88-bits each
10: Calculate the count of 1's for each byte X[x1;x2;...;x8] as well as the count of 1's for each 11 bits Y[y1;y2;...;y8 inp2]
11:forj=1;2;...;Qdo
12:a= Con {d;Y[i] }, where Con is the concatenation function.
13:d=p1 sj
14:d= Perm {d;X[i] }, where Perm is the permutation function.
15:Plain[j] =d
16:end for
17: Return the plaintext Plain [m1;m2;m3;...;mQ] , where mj is the plaintext of SNj
18:end for.

5. Performance Evaluation and Analysis

To Implement the Proposed hybrid approach using NS2, the Simulation parameters are initialized as shown in table1. The performance of E-AODV is analyzed with AODV by considering the parameters throughput, Load Balancing, End to End Delay, Energy consumption, Delivery ratio, and Energy consumption.

Throughput reflects the delivery rate of packets transmitted within the Time Interval. Better throughput imposes high performance.

End to end delay projects the average time-lapsed which shows delay during transmission between source and destination.

Packet Delivery Ratio is defined as the proportion measured within packets delivered and packets received at the destination.

Load Balancing is the efficient sharing of traffic among networks in several environments fulfilling data transmission.

Energy Consumption is defined as the amount of energy consumed or depleted during transmission with battery-powered nodes.

Table 1: Simulation Parameters

PARAMETERS	VALUES
Simulator	NS2
Simulator Time	100 s
Simulation Area	1000*1000 m
Proposed Protocol	Enhanced AODV (hybrid approach)
Initial Energy of nodes	1J
Number of Nodes	Variable up to 100
Bit Rate	1Mb/sec
Packet Length	600 byte

Observations :

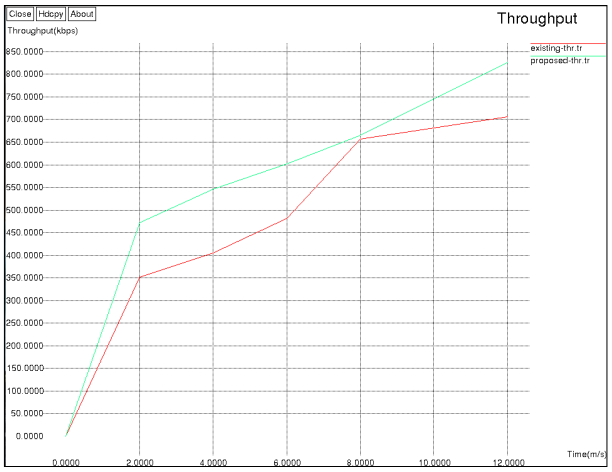

Fig 1. Throughput of AODV Vs E-AODV

The proposed schema is compared with AODV as shown in fig 1, and uncovered results promised increased throughput on the scale of X graph with a green spike for E-AODV and red spike for AODV.

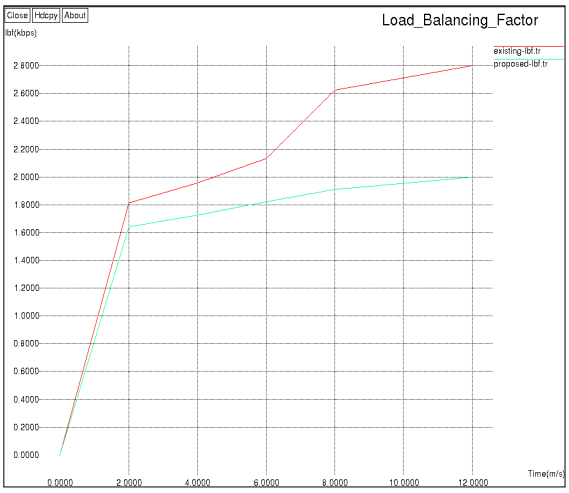

Fig 2. Load Balancing of AODV Vs E-AODV

The proposed approach is compared with AODV as shown in fig 2, and achieved results promised improved throughput on the scale of X graph with a green spike for E-AODV and red spike for AODV.

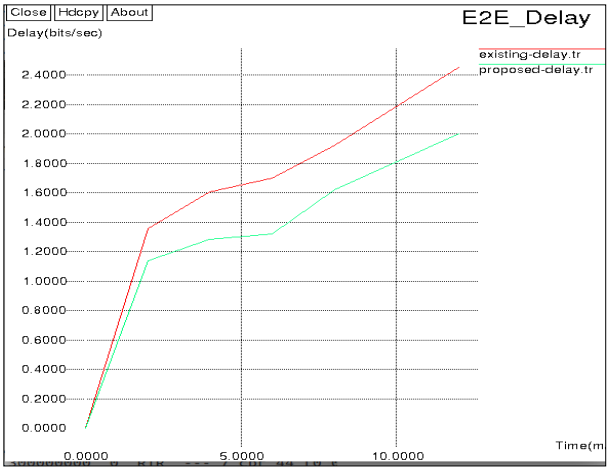

Fig 3. E2E of AODV Vs E-AODV

The proposed approach is studied against AODV as shown in fig 3, and profound results promised declined delay on the scale of X graph with a green spike for E-AODV and red spike for AODV.

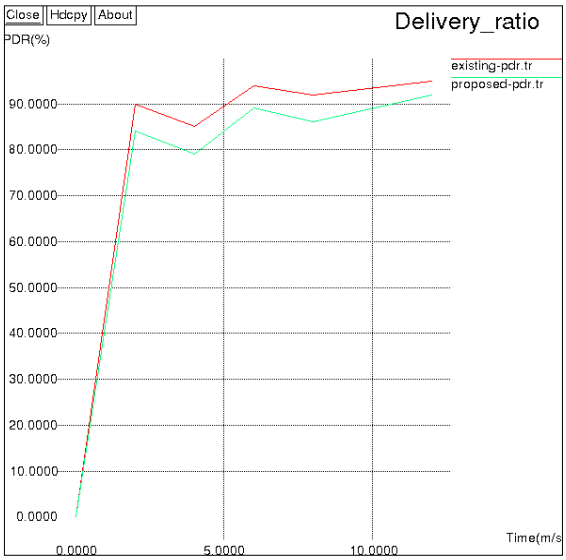

Fig 4. Delivery Ratio of AODV Vs E-AODV

The proposed approach is compared with AODV as in fig 4, and obtained results promised increased delivery ratio on the scale of X graph with a green spike for E-AODV and red spike for AODV.

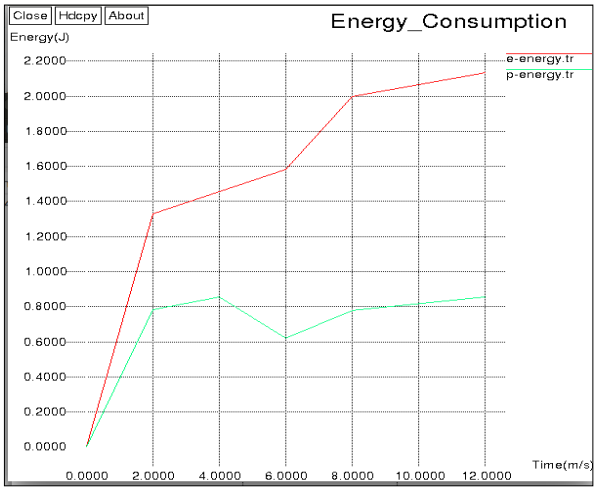

Fig 5. Energy Consumption of AODV Vs E-AODV

In our proposed schema we compared energy consumption with AODV as shown in fig 5, and obtained results promised lowered energy consumption on the scale of X graph with a green spike for E-AODV and red spike for AODV.

6. Conclusion

Our approach promises to address the entailing hindrance aspects in AODV like collision, energy consumption, and security [14]. The proposed E-AODV approach successfully handles collisions by introducing Mobile Sink, reducing the energy consumption with GAF, and enhancing the security aspects like authentication, confidentially and integrity using homomorphic encryption. This enhanced version renders leveraged scope for MANET's application domain in circumstances where battery life, transmission rate, privacy, and performance are of utmost concern. It even offers a challenge for future enhancements in these fore mentioned parameters with technology evolving concurrently with network needs.

References

[1] Anguraj, D. K., & Smys, S. Trust-Based Intrusion Detection and Clustering Approach for Wireless Body Area Networks. Wireless Personal Communications.Volume 120, pp. 1-20,2018. DOI:10.1007/s11277-018-6005-x .

[2] Asad Amir Pirzada and Chris McDonald, Secure Routing with the AODV Protocol Asia-Pacific Conference on Communications, Perth, Western Australia, 2005, pp 57-61,3 – 5.

[3] Awadhesh Kumar and R. R. Tewari, Symmetric Key Cryptography based Secure AODV Routing in Mobile Adhoc Networks, Advances in Wireless and Mobile Communications. ISSN 0973-6972 Volume 10, pp. 969-984,2017

[4] Belghith, A., Belhassen, M., Dhraief, A., Dougui, N. E., & Mathkour, H. . Autonomic Obstacle Detection and Avoidance in MANETs Driven by Cartography Enhanced OLSR. Mobile Information Systems, pp 1–18,2015

[5] Chen, B., Jamieson, K., Balakrishnan, H., & Morris, R. Span An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks. Proceedings of the 7th Annual International Conference on Mobile Computing and Networking - MobiCom '01. DOI:10.1145/381677.381686, vol:8,pp 481-494,2002

[6] Deepak.S, & Anand. H, AODV Route Discovery and Route Maintenance in MANETs. 5th International Conference on Advanced Computing & Communication Systems (ICACCS). DOI:10.1109/icaccs.2019.8728456 ,2019

[7] Grover, J., Shikha, & Sharma, M.. Optimized GAF in Wireless Sensor Network. Proceedings of 3rd International Conference on Reliability, Infocom Technologies, and Optimization,2014

[8] Gupta, A., & Rana, K. Assessment of various attacks on AODV in a malicious environment. 2015 1st International Conference on Next Generation Computing Technologies (NGCT). DOI:10.1109/ngct.2015.7375103,2015

[9] Keshavarz, H., Noor, R. M., & Mostajeran, E. Using the Routing Table Flag to Improve Performance of AODV Routing Protocol for VANETs Environment. Advances in Intelligent Systems and Computing, 73–82. DOI:10.1007/978-3-642-37371-8_11,2013

[10] Liu, S., Yang, Y., & Wang, W. Research of AODV Routing Protocol for Ad Hoc Networks1. AASRI Procedia, vol 5,pp 21–31. DOI:10.1016/j.aasri.2013.10.054,2013.

[11] Mafirabadza, C., & Khatri, P. Efficient Power Aware AODV Routing Protocol for MANET. Wireless Personal Communications, 97(4), 5707–5717. DOI:10.1007/s11277-017-4804-0 ,2017

[12] Mittal, S., Kaur, R., & Purohit, K. C. Enhancing the data transfer rate by creating an alternative path for the AODV routing protocol in VANET. 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall),2016

[13] Parmar, M. K., & Jethva, H. B. Analyze the impact of malicious behavior of AODV underperformance parameters. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies,DOI:10.1109/icaccct.2014.7019184,2014

[14] Rajan Patel, Pariza Kamboj, A Novel Key Distribution Scheme for Link Encryption in MANET, A novel key distribution scheme for link encryption in MANET. Journal of Mobile Computing, Communications & Mobile Networks; 2(3): pp 59–72,2015

[15] Ray, N. K., & Turuk, A. K. A Hybrid Energy Efficient Protocol for Mobile Ad Hoc Networks. Journal of Computer Networks and Communications, pp 1–11. DOI:10.1155/2016/2861904,2014

[16] Sinchan Roychowdhury, and Chiranjib Patra, Geographic Adaptive Fidelity and Geographic Energy-Aware Routing in Ad Hoc IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5

[17] Spurthi. K, and T N Shankar, An Efficient Cluster-Based Approach to Thwart Wormhole Attack in Adhoc Networks, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 9, 312,2020

[18] Spurthi. K, Srinivasarao Tammireddy, Satyabrata Patro, T. N. Shankar, G. Swain and Ranjan K. Senapati, Far East Journal of Electronics and Communications Volume 16, Issue 3, Pages 511 - 525, 2016

[19] Spurthi. K and NarayanShankar T. A Survey of Intrusion Detection System in Manets using Security Algorithms, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 pp. 14408-14414, Research India Publications,2017.

[20] Srinivasa P, Murthy, Sainath P, Vishnu J, Packet Collision Avoidance in Energy Efficient CCMANETs International Journal of Latest Technology in Engineering, Management &Applied Science (IJLTEMAS) Volume VIII, Issue IV, April | ISSN 2278-2540,2019

[21] Sun, X., Yu, F. R., Zhang, P., Xie, W., & Peng, X. A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks,vol 20(15),2020

[22] Xinlian, Z., & Zepeng, Z. . An improved GAF routing algorithm. 3rd IEEE International Conference on Computer and Communications (ICCC).DOI:10.1109/compcomm.2017.8322542,201

[23] Xu, Y., Heidemann, J., & Estrin, D. Geography-informed energy conservation for Ad Hoc routing. Proceedings of the 7th Annual International Conference on Mobile Computing and Networking MobiCom '01. DOI:10.1145/381677.381685,2001

[24] Ziwei, Y., Amrit, M., Lixia, Y., Sidheswar, R., & G, P. . Energy-efficient node positioning in optical wireless sensor networks. Optik. DOI:10.1016/j.ijleo.2018.09.186 ,vol 178.pp 461-466,2018

[25] G Pradhan, A., Raja Sekhar, K., Swain,Digital image steganography combining lsb substitution with five-way PVD in 2×3 pixel blocks, International Journal of Pharmacy and Technology 8 (4), pp.22051-22061,2017.

[26] KR Sekhar, LSS Reddy, UJ Kameswari,Secure system of attack patterns towards application security metric derivation, International Journal of Computer Applications 53 (1), pp.11-18,2012.

[27] Krovi Raja Sekhar, Veerapaneni, S.S., A systematic study of asset management using hybrid cyber security maturity model, International Journal of Recent Technology and Engineering 7 (6), pp. 140-145, 2020.

K. Spurthi received her B.Tech(CSE) from Adams Engineering College, Khammam and M.Tech(CSE) at Swarna Bharathi Institute of Science and Technology Khammam, AP, India. She is pursuing Ph.D(CSE) at KL University, Guntur Dist AP, India. She has 3 reputed journals in her credit. Her research interest is “Development of security system in MANET's”

T. N. Shankar obtained his M. Tech and Ph.D degree in Computer Science & Engineering from Birla Institute of Technology, Mesra, Ranchi, India. He has been working as Professor in CSE, KL University, Guntur, AP, India, since 2015. He has about 30 reputed journals and 8 conference papers to his credit. His research interests include information security and neural networks, and he has published a book on neural networks.