

A Survey on Node Capability Based Trusted Routing in MANET: Issues & Challenges

Mohan Patsariya¹,

Department of Computer Science & Engineering
Shri Vaishnav Vidyapeeth Vishwavidyala
Indore, India
e-mail: mohan.patsariya@gmail.com

Anand Rajavat²

Department of Computer Science & Engineering
Shri Vaishnav Vidyapeeth Vishwavidyala
Indore, India
e-mail: anandrajavat@yahoo.co.in

Abstract— *Now a day's mobile ad-hoc network is gaining popularity due to system application demands such as internet of things (IoT) based sensor deployment, home surveillance system, atmospheric emergency data gathering, Ad-hoc hotspot communication establishment etc. The new generation of communication focuses to handle the entire electronic devices through sensor with lightweight processes model (LWP) for real time data acquisition and monitoring. In this paper we analyze research gap in existing schemes with issues and challenges towards the efficient path selection with trusted communication which provides the strength to the new age of communication technology. This paper explores various aspects of capability based trusted routing scheme in Mobile Ad Hoc Network for improvising the network performance.*

Keywords—*MANET; Node Capability; Selfish Node; Trusted- Secured Routing;*

I. INTRODUCTION

A mobile ad hoc network (MANET) consists of a group of mobile nodes (MNs) that communicate with each other without the presence of infrastructure [1]. MANETs are used in various applications of disaster recovery, and also used for rescue operations & military communication and in many other applications. In respect to provide data communication throughout the network, the mobile nodes must design to handle the different network functions, such as packet routing etc. The wireless mobile hosts communicate in a manner of multi hop fashion. In multi-hop wireless ad-hoc networks, it is critical to design efficient routing protocols since mobile nodes have very limited battery power or energy, computing power and communication capabilities [2]. The challenging task in these ad hoc networks is to find

and develop routing protocols that can efficiently find routes between any two nodes. Mobile ad-hoc network is a tremendous way of communication in small geographical areas for short period of time. It provides new age to communication because they form network without stable routing, where each node is capable to make routing table and routing decision in independent manner [3].

II. BACKGROUND

In this section we present some basic concept in order to help to understand the paper's contributions. Initially we present concept of selfish nodes, need of trust & trust calculation in MANET and finally the node capacity.

A. Selfish Nodes

Intermediate nodes in MANET help each other to forward packets. The nodes are expected to wait for pre set interval of time, but due to congestion of network and selfishness mobile node may misbehave. Misbehavior of nodes is generally defined as deviation from original routing and forwarding [4].

The selfish node does not participate in routing, which results in delay and packet drop. The selfish node utilizes its limited resources for its own purpose because of energy constraint in MANET. Selfish nodes expects to spare its resources to the most extreme, so these nodes disposes of every single approaching packets, these nodes disregard to share the resources like battery control, memory space, CPU Time to alternate nodes. The misbehavior of nodes is well observed when the mobile nodes possess low residual power in data link/ MAC Layer. The main features of selfish nodes:

- Packet dropping
- No participation in routing process
- No transmission/ No reply to HELLO message

B. Need of Trust

In general the "Trust" is known as the "degree of belief (subjective)" about behavior of an individual entity [4]. Blaze et al. [5] initially presented the expression "Trust" and distinguished it as a different segment of security benefits in systems and illuminated that "Trust gives a bound together way to deal with indicating and translating security strategies, accreditations, and connections." Trust calculation in MANETs is required while participating nodes, with no past associations, want to set up a system with a worthy level of trust among themselves [6].

Mobile ad-hoc network is more vulnerable as compare to other existing network because in decentralized based communication no one is responsible to manage the historic database while the nodes are dynamic and move inside the network and form temporary communication. MANET faces problems from various attack i.e. black-hole, gray-hole, wormhole etc.

Trust calculation and detection of selfish node is an important issue, it is also important to focus on the energy value of each node by reducing the consumption using various routing protocol. For the detection of misbehaviour of intermediate nodes, trust analysis is an important factor [7] [8][9]. In MANET, trust is a challenging task to achieve secure

communication between nodes. Some of researcher calculates the trust through various methodologies described in section of related work.

C. Node Capability

Mobile Ad Hoc Network capability depends on mobile device and communication links; it means whole mobile ad hoc communication is device and channel dependent. Node capability depends on processing capacity, memory or queue capacity, power requirement for data transmission; receiving etc. on another side link capacity depends on channel bandwidth and frequency.

III. RELATED WORK

In this section, we present numerous research work done for improvising the ad-hoc communication and to solve various upcoming challenges before making applicable to real-time implementation.

A. Different Path selection Mechanism

I. Alagiri, T. Muthamil Selvan et al [10] proposed a multi-path routing algorithm that selects multiple paths with minimized control overhead, the different multi-path selection approach to be carried out in three method called multipath, stable multipath, and short stable multipath. Link stability between more than few nodes in the select path is considered between those minimum value path stability because of a path is not strong compare to weakest link.

Sameer Abdulateef Hussein, Dahlila Putri Dahnli [11] proposed a new hybrid technique to improve the path selection and reducing Energy Consumption in MANET. The Authors describes and introduces a new technique for improving path selection by combining two types of techniques i.e. ant-colony optimization and lion optimization algorithm and then all possible paths were discovered in the network. This technique improves the energy efficiency and actual path selection or improves the performance metrics of each node.

Taha A., Alsaqour R., Uddin M., Abdelhaq M., Saba T et al [12] proposed the fitness function technique for energy consumption in MANET, this technique also optimize the energy consumption in (AOMDV) routing protocol. The proposed protocol is called AOMDV with the fitness function (FF-AOMDV). To reduce the energy consumption in multipath routing protocol with used fitness function finds the optimal path from source node to destination node. Using the NS2 performance has been evaluated of the proposed FF-AOMDV protocol, behavior of

two protocols compared with the performance of ad-hoc on demand routing protocol and with life maximization (AOMR-LM) protocols. The comparison was evaluated based on different parameters like energy consumption, throughput, packet delivery ratio, end-to-end delay, network lifetime and routing overhead ratio performance metrics, variation in node speed, packet size, and simulation time.

P.E.Irin Dorathy, Dr.M.Chandrasekaran [13] describes the distance based dual Path Ad Hoc on Demand Distance Vector Routing Protocol. The new technique is a novel method for selecting an optimal path between the nodes for data transmission in MANET. Routing is important issues in MANET, normally selection of the path were based on different type of parameter like distance between the nodes, hops count, delay, trust values, residual energy, received signal strength etc. In proposed method considering the distance metric optimal route is selected out of discovered two routes for data transmission. Simulation for proposed routing protocol results in high packet delivery ratio with less average end to end delay and low routing overhead.

Calduwel Newton Pitchai, Nismon Rio Robert [14] proposed a path selection method PSA-HD: Path Selection Algorithm based on Hamming Distance to Enhance the Link Stability in MANET. In the proposed scheme two different conditions are identified, first condition is link failure identification, and second is stable link selection from the available links to reach the destination and determines a stable path. Simulation result shows that, there is a decrease in average End-to-End delay and increase in Packet Delivery Ratio (PDR).

Ejmaa, Ali Mohamed E., et al [15] proposed a scalable neighbor based routing protocol; in this scheme broadcasting is controlled through inverse relation between number of neighbor and probability of rebroadcasting of route request message. Based on simulated result author conclude that, the proposed scheme performs well in terms of routing overhead, medium access control collision, end-to-end delay, packet delivery ratio and consumption of energy.

B. Different Capability Based Model/Routing

Dagade, Mr Veershetty M [16] proposed Capability based routing (CBR) with flow control, admission control, policy control mechanism. The proposed system is robust against variety of threats (multi hop) and performs well over the range of different scenarios.

Jabbar,Waheb A., Mahamod Ismail, Rosdiadee Nordin [17] Proposed a scheme based on multi criteria node rank metric i.e. battery energy and node speed. The proposed multipath battery and mobility aware routing scheme is based on link assessment function to select the most efficient stable path between intermediate nodes.

Roy, Sarbani, Dhrubajyoti Chatterjee, Nandini Mukherjee [18] proposed a routing scheme namely capability aware ad-hoc routing algorithm, this scheme is useful for gathering information pertain to node capability during route discovery and use this information in node selection to find the best route to that node.

Vhora, Sumaiya, Rajan Patel, Nimisha Patel [19] Investigated and proposed the rank based data routing scheme; this scheme is used to identify the node behavior in network. The proposed scheme is useful for the identification of malicious path and prevents the packet drop attack.

Farkas, Károly, et al [20] proposed a Node weight scheme (NWC), this scheme is useful for computing the weight of node, and the priority of node is decided by taking into consideration of several parameters for weight computation and optimization. The proposed scheme can also be used in case of cluster algorithm design.

Sivakumar, B., G. Varaprasad [21] put efforts through considering randomly connected nodes which can fail at random. The author proposed a scheme to detect the critical node based on energy, reliability, traffic type and bandwidth. The performance of proposed scheme has been evaluated based on end-to-end delay and throughput.

Ahmed A. Radwan, Tarek M. Mahmoud, Essam H. Houssein [22] compares the important parameters like routing messages overhead, throughput and end to end delay. Using parallel discrete - event simulator show the performance of various protocols like AODV, LAR and FSR. In case of end to end delay LAR outperforms and AODV shows high throughput.

G.S. Mamatha, Dr.S.C. Sharma [23] suggested that, it is important to analyze the quantitative behavior and implementation issues in MANET environment, like transmission of radio range and Battery life, speed of movement and processing capacity of different nodes. Several analytical models have been developed so far to describe the behavior, but they are restricted in several aspects.

Pavel Polak, Róbert Drlicka, Ján Žitnansky [24] discussed that capability assessment of device is an important process of quality control. Various performance metrics were used for capability assessment of devices.

Kelothu Yakhoob Mrs.B.Dhanalaxmi K. Shanthi Priya [25] proposed (COCO) capacity –optimized Cooperative topology scheme for improving the network capacity in MANET with cooperative communications, jointly by considering both upper layer capacity and physical layer co-operative communications.

R. Menaka, V. Ranganathan, B. Sowmya [26] Proposed scheme is to investigate the performance of DSR under untrustworthy environment. The proposed model is fuzzy based and calculate the total trust value and mobility of nodes. Scheme mainly focus on parameters used in secured route design for data transmission in the network. On comparison with DSR protocol in untrustworthy environment, the proposed scheme shows improved quality of services.

C. Different Trust Calculation scheme

Ashish Kumar Jain, Vrinda Tokekar [27] proposed a trust computing scheme using fuzzy based max-product composition for determining the malicious nodes and safe route in MANET through compute aggregated trust values. As per scheme, proposed protocol shows performance improvements over AODV protocol and analyzed network parameters under different mobility conditions and different positions of black hole nodes.

Muhammad Salman Pathen, Nafei Zhu, Jingsha He [28] proposed a QoS route selection through combination of social and QoS trust. The proposed scheme is to check activities of various forwarding packets and on discovering the path ensures reliable communication through the trust mechanism. Scheme is useful for the selection of best forwarding node capability in terms of QoS parameters, such as residual energy, channel quality, link quality, etc. The proposed scheme is an adversary model for packet dropping attack and analyzed using network simulator-2 (NS2) under various network conditions. The result shows that combination of social and QoS trust parameters improves security and quality of service routing in terms of overhead, packet delivery ratio or energy consumption.

Pooja Pilankar, Puja Padiya [29] has analyzed different proposed trust based mechanism and trust

evaluation based security solution. These techniques are useful to make more effective trust security solutions. It is suggested that behavior of node is calculated in the form of numerical value called trust.

Gayathri Dhananjayan, Janakiraman Subbiah [30] proposed scheme based on trust awareness for the improvement of trust level amongst the nodes in Mobile Ad Hoc networks. The scheme significantly modifies the conventional AODV routing protocol with the different type of constraints of trust rate, energy, and mobility based malicious behavior prediction. The trust level calculation is based on; the direct and indirect trust observation. The proposed scheme analyzed with the existing methods on different parameter the average end-to-end delay; throughput, false positives, and packet delivery ratio.

Ankit Agrawal, Dr. A.K.Verma [31] discussed the concept, properties and unique characteristics of trust in MANET. Further, an analysis of possible attacks in MANET is also done. A survey on the trust management methods developed for MANET is provided with future research direction in trust management in MANET.

Kotari Sridevi, Dr. M. Sridhar [32] proposed an approach for node trust computation for the improvement in the quality of service. It computes individual node trustworthiness based on node throughput and packet drop during communication. It prevents the network from abnormal and malicious nodes to improve the security and throughput. The evaluation measures to improvement in throughput with less packet drop and computational overload in compare to existing protocols.

Jan Papaj, Lubomir Dobos [33] suggested that the main problems of all networks occur if the communication paths are disconnected for a short time. For communication between isolated islands with limited connectivity, the main issue is in selection of reliable path and trusted nodes. The relay node selection is also critical factor as data are transmitted in hostile environment. As per scheme two algorithms were introduced for trust based relay node selection, when connections are disrupted these algorithms will become activated. The proposed algorithms enable selecting reliable relay nodes based on collecting routing information and contact history and introduce the network performance analyses of these algorithms

Borkar, Gautam M., Anjali R. Mahajan [34] proposed a technique based on security aware dual authentication using fuzzy logic to choose the most

efficient path and also incorporate cipher policy based encryption with game theory based attack model.

Hemamalini, V.G. Zayaraz, V.Vijayalakshmi [35] proposed a scheme using adaptive fuzzy logic to provide solution for detection of malicious node. The proposed scheme is an enhancement trust management model incorporated over ad-hoc on demand distance vector (AODV) routing protocol to meet the security parameter. The proposed scheme investigated in terms of productivity and viability of proposed model.

Anusha, K., E. Sathiyamoorthy [36] proposed a trust based authentication routing with bio-inspired intrusion detection system by combining the concept of deep packet inspection and trust, the security can be improved by using public key or private key pair for initiating route and authentication is based on trust of node. The experimental result shows the performance in terms of delivery ratio, delay, security cost, and misdetection.

Qin, Danyang, et al [37] proposed a trust sensing-based secure routing mechanism (TSSRM) with the lightweight model. The scheme consist of the different steps and process like network initialization process based on the concept that higher the trust degree, higher its energy is and longer the node lifetime. Further scheme follows the Route construction process, Route maintenance methods, with this simulation result shows that routing overhead is minimized with this scheme and improves the reliability of data transmission compared with traditional mechanism.

Anita, X., M. A. Bhagyaveni, J. Manickam [38] proposed fuzzy based (FTPR) scheme for trust prediction model for routing in wireless sensor network with minimum overhead and energy consumption. The proposed scheme predicts the future behavior of neighbor node based on the history of node. The scheme is recommendation based trust calculation model in which group of nodes (subset) receives recommendation with node who had maximum number of interaction with requester node. The analysis result shows that proposed protocol gives high packet delivery ratio, network lifetime, and low end-to-end delay with low consumption of energy.

Bisen, Dhananjay, Sanjeev Sharma [39] proposed an agent based secure approach for performance enhancement of MANET, based on optimal node reliability factor agent nodes is chosen. The reliability factor is calculated through node performance feature like normalized distance value, mobility and degree difference. A process of malicious node detection

using fuzzy based approach is performed with comparative analysis through conventional schemes based on packet delivery ratio, throughput, network overhead etc.

Abbas, Nihad I., Mustafa Ilkan, Emre Ozen [40] proposed a fuzzy based trust scheme to enhance the performance of on demand distance vector (AODV) through selection of trusted nodes. The node parameters taken into consideration, such as residual energy. Node mobility, number of hop to check the trust value of node for construction of optimal path. The simulation analysis shows that the proposed scheme works well as compared to traditional AODV.

IV. ISSUES AND CHALLENGES

Mobile Ad Hoc Network device execute functions under limited resources such as battery power, processing power and memory size because, they are portable as well as movable devices. For data transmission in MANET, the wireless channel capacity and frequency is also limited. Therefore routing scheme is important in network for communication, in the past decades of research various routing schemes were proposed for route selection between sources to receiver. Based on previous research and literature survey, we analyze some issues and challenges in this section.

A. Node Capability

As mobile network nodes are low capable devices and if we send data without capability measurement of nodes then data cannot be handled by intermediate nodes which causes the data dropping and unnecessarily channels are busy.

B. Resource Utilization Monitoring

The monitoring of resource utilization is also important for providing fairness services to the end users and it helps to shift the load of highly loaded node to lightly loaded node so that response time delay is minimized.

C. Trust Measurement

Calculation of trust mechanism is very essential for the mobile ad-hoc network due to node mobility and decentralized controlling system which cannot store the communication information in a single device, so the trust calculation is more beneficial for this type of communication structure. In the dynamic topology if some of the nodes do not follow the protocol and flood unwanted data in the network or modified the routed

data, those data are harmful for the overall communication backbone, so these networks requires the strategies to monitor and calculation of trust value of nodes in path selection for the better services.

Based on reported issues and available literature, it is clear that MANET has scope of research for secured and trusted routing. Trust calculation is very important for dynamic network because node's behavior and network structure changes frequently and past history as well as new activities of nodes are useful for data transmission.

Capable and stable path selection is an essential requirement in MANET for better network performance. So node capability checking has wide scope of research in stable network designing. Therefore, to improve the network performance with stable and secured network, there is a need to develop a new capability based trusted routing scheme in Mobile Ad Hoc Network

Table 1: Research Gap analysis of existing schemes

Author, Publication, Year	Research Gap
Sharma,J.,Baghel, A.S., Proceedings of International Conference on Recent Advancement on Computer and Communication. SPRINGER, 2018	The given technique only deals with the congestion issues in the network.
Farkas, Károly, et al., 16 th IEEE International Conference on. Computer Communications and Networks, ICCCN, 2007	The proposed approach to create the service profile does not predict the network scenario, mobility behavior of nodes in advance.
Sivakumar, B., G. Varaprasad, International Journal of Advanced Computer Science and Applications” IJACSA Vol- 3 No.1 , 2012	The scheme deals only with the identification of critical nodes based on residual battery power, service traffic type, and bandwidth.
G. S. Mamatha, S. C. Sharma, International Journal of Computer Science & Engineering Survey (IJCSSES) 1.1, 2010	Authors are not suggesting a specific technique to work and enhance the quality of network.

R. Menaka et al., Wireless Personal Communications 94.4, 2017	Authors worked on the performance issue in DSR protocol and not considering the issue of capacity of network and mobile nodes.
Ashish Kumar Jain, Vrinda Tokekar, Oriental Scientific Publishing March 2017, Vol. 10, No. (1)	Authors are not concerned to deal with the capacity of nodes, only security enhancement is considered.
Sridevi, K., Sridhar, M., International Journal of Intelligent Engineering and Systems, Vol.10, No.6, 2017	Proposed scheme can build more stable networks by analyzing the semantic changes in the negative and positive message spread by reliable and malicious node.
Dhananjayan G, Subbiah J., Springer Plus., 2016	The security can be enhanced using location key management protocol.
Abbas, Nihad I., Mustafa Ilkan, and Emre Ozen, EURASIP Journal on Wireless Communications and Networking, 2015	In proposed scheme more factors and metrics may be considered in fuzzy inference engine to enhance the route selection decision making.
Qin, Danyang, et al., IEEE Access journal, 2017	In proposed scheme, distributed intrusion detection may provide a new way of research of trust degree.

V. CONCLUSION

Mobile ad-hoc network is a resource constraint device but in recent trends of communication it is very useful for the hotspot communication between devices and internet of thing technology. MANET device are capable to form route and provide services to other

mobile device and cost less communication. In Mobile Ad Hoc Network, node trust and link trust calculation is difficult because of random change in the network topology and communication provider nodes.

References

- [1] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989. Mohammad A. Mikki "Energy Efficient Location Aided Routing Protocol for Wireless MANETs"; *International Journal of Computer Science and Information Security (IJCSIS)* Vol. 4, No. 1 & 2, ISSN: 1947-5500, 2009, pp. 59-67.
- [2] M. Rehan Rasheed, M. Kamran Khan, M. Naseem, Aisha Ajmal and Ibrahim M. Hussain "Performance of Routing Protocols in WiMAX Networks", *IACSIT International Journal of Engineering and Technology*, Vol.2, No.5, ISSN: 1793-8236, 2010, pp. 412-417.
- [3] Subir Kumar Sarkar, T G Basavaraju, C Puttamadappa "Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications", Auerbach Publications Taylor & Francis Group, ISBN-13: 978-1-4200-6221-2, 2008, pp. 349.
- [4] K. S. Cook (editor), *Trust in Society*, vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York, ISBN: 978-0-87154-181-9, pp. 432.
- [5] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proc. IEEE Symposium on Security and Privacy*, 6-8 May, 1996, pp. 164 - 173.
- [6] R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks," *Proc. IEEE GLOBECOM*, San Francisco, CA, Dec. 2003, pp.1511- 1515.
- [7] L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," *Proc. 10th Int'l Security Protocols Workshop*, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.
- [8] Chaurasia BK, Tomar RS (2012) "Trust management model for wireless ad hoc networks". In: Deep K, Nagar A, Pant M, Bansal CJ (eds) *Proceedings of International conference on soft computing for problem solving (SocPros 2011)* December 20-22, 2011, vol 1. Springer, Newdelhi, pp. 201-2016.
- [9] Dhananjayan G, Subbiah J. T2AR: trust-aware ad-hoc routing protocol for MANET. *SpringerPlus*. 2016;5(1):995. doi:10.1186/s40064-016-2667-6, pp. 1-16.
- [10] I. Alagiri, T. Muthamil Selvan, P. Thenapal and C. Navaneethen "Stable Multipath Routing Protocol using Different Route Selection Mechanism for Mobile Ad-hoc Networks" *IJPAM* Volume 117 No. 15 2017, pp. 25-40 .
- [11] Sameer Abdulateef Hussein and Dahlila Putri Dahnil "A New Hybrid Technique to Improve the Path Selection in Reducing Energy Consumption in Mobile AD-HOC Networks" *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 12, Number 3 (2017) pp. 277-282.
- [12] Taha A., Alsaqour R., Uddin M., Abdelhaq M., Saba T, Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function (2017) *IEEE Access*, 5 , art. no. 7933071, pp. 10369-10381.
- [13] Dorathy, P. I., & Chandrasekaran, M. (2017, January). Distance based dual path ad hoc on demand distance vector routing protocol for mobile ad hoc networks. In *Advanced Computing and Communication Systems (ICACCS)*, 2017, IEEE, pp. 1-6.
- [14] Calduwel Newton Pitchai, Nismon Rio Robert "PSA-HD: Path Selection Algorithm based on Hamming Distance to Enhance the Link Stability in Mobile Ad-hoc Networks" Received: September 12, 2017 *International Journal of Intelligent Engineering and Systems*, Vol.11, No.1, 2018, DOI: 10-22266/ijies2018.0228.27, pp. 259-266.
- [15] Ejmaa, Ali Mohamed E., et al. "A scalable neighbor-based routing protocol for mobile ad hoc networks." *International Journal of Distributed Sensor Networks* Vol.12(9) (2016): 1550147716665501, pp. 1-12.
- [16] Dagade, Mr Veershetty M. "Capability Based Routing With Security Using Mobile Agents And Threat Locator Mechanism In Wireless Mesh Network." (2014), *IJAICT* Vol. 1, Issue -3, ISSN: 2348 – 9928, pp. 372-378.
- [17] Jabbar, Waheb A., Mahamod Ismail, and Rosdiadee Nordin. "Energy and mobility conscious multipath routing scheme for route stability and load balancing in MANETs." *Simulation Modelling Practice and Theory* 77 (2017): pp. 245-271.
- [18] Roy, Sarbani, Dhrubajyoti Chatterjee, and Nandini Mukherjee. "Capability aware routing algorithm for Mobile Ad-Hoc Network in workplace." *Networks, 2008. ICON 2008. 16th IEEE International Conference on*. IEEE, 2008, pp. 1-6.
- [19] Vhora, Sumaiya, Rajan Patel, and Nimisha Patel. "Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET." *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on*. IEEE, 2015, pp. 1-5.
- [20] Farkas, Károly, et al. "NWC: node weight computation in MANETs." *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*. IEEE, 2007, pp. 1059 – 1064.
- [21] Sivakumar, B., and G. Varaprasad. "Identification of critical node for the efficient performance in Manet." *International Journal of Advanced Computer Science and Applications" IJACSA Vol- 3 No.1* (2012), pp. 166-171.
- [22] Radwan, Ahmed A., Tarek M. Mahmoud, and Essam H. Houssein. "Performance measurement of some mobile ad hoc network routing protocols." *International Journal of Computer Science Issues (IJCSI)* 8.1 (2011): pp. 107 -112.
- [23] Mamatha, G. S., and Dr SC Sharma. "Analyzing the MANET variations, Challenges, Capacity and protocol issues." *International Journal of Computer Science & Engineering Survey (IJCSES)* 1.1 (2010): pp. 14-21.
- [24] Polák, Pavel, Robert Drlička, and Ján Žitňanský. "Capability assessment of measuring equipment using statistic method." *Management systems in production engineering* 4 (16) (2014): pp. 184-186.
- [25] Kelothu Yakhoob, B.DHANALAXMI K. SHANTHI PRIYA "Capacity Optimized Cooperative Topology Control in Mobile Ad Hoc Networks with Cooperative Communications" *IJEEE* Volume 1, Issue 9, September 2014. ISSN: 2348-4748, pp. 18-21.
- [26] Menaka R., V. Ranganathan, and B. Sowmya. "Improving Performance Through Reputation Based Routing Protocol for Manet." *Wireless Personal Communications* 94.4 (2017): pp. 2275-2290.
- [27] Ashish KumarJain, and Vrinda Tokekar, "Security Enhancement of AODV Protocol using Fuzzy based Trust Computation in Mobile Ad Hoc Networks" *Oriental Scientific Publishing* March 2017, Vol. 10, No. (1): Pgs. 94-102.
- [28] Pathan, Muhammad Salman, et al. "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs." *Future Internet* 10.2 (2018): pp. 1-16.
- [29] Pooja Pilankar, Puja Padiya "Trust based security in manet" *IJRET: International Journal of Research in Engineering and*

Technology Volume: 05 Issue: 02, Feb-2016, ISSN: 2321-7308, pp. 1-7.

- [30] Dhananjayan, Gayathri, and Janakiraman Subbiah. "T2AR: trust-aware ad-hoc routing protocol for MANET." *SpringerPlus* 5.1 (2016): pp. 995.
- [31] Ankit Agrawal, Dr. A.K.Verma, "A review & impact of Trust Schemes in MANET" AICTC Proceedings of International conference on Advances in Information Communication Technology & Computing, Article No. -26, 2016, ISBN: 978-1-4503-4213-1, pp. 1-7.
- [32] Sridevi, K., & Sridhar, M., "A Reliable Trustworthy Approach Based on Node Behavior Prediction for Secure Routing in MANET", International Journal of Intelligent Engineering and Systems, Vol.10, No.6, 2017 DOI: 10.22266/ijies2017.1231.25, pp. 230-241.
- [33] Jan Papaj and Lubomir Dobos "Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN" Research Article Received 4 January 2016; Revised 8 March 2016; Accepted 23 March 2016. SCI Vol(2016), Article ID 7353691, <http://dx.doi.org/10.1155/2016/7353691>, pp. 1-18.
- [34] Borkar, Gautam M., and Anjali R. Mahajan. "Security Aware Dual Authentication based Routing Scheme using Fuzzy Logic with Secure data Dissemination for Mobile Ad-hoc Networks." *Journal of Applied Security Research* 13.2 (2018), pp. 223-249.
- [35] Hemamalini, V., G. Zayaraz, and V. Vijayalakshmi. "An Enhanced Trust Management Framework for MANET using Fuzzy Prediction Mechanism." *International Journal of Security and Its Applications* 9.1 (2015): pp. 11-24.
- [36] Anusha, K., and E. Sathiyamoorthy. "A new trust-based mechanism for detecting intrusions in MANET." *INFORMATION SECURITY JOURNAL* 26.4 (2017): pp. 153-165.
- [37] Qin, Danyang, et al. "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network." *IEEE Access* 5 (2017): pp. 9599-9609.
- [38] Anita, X., M. A. Bhagyaveni, and J. Manickam. "Fuzzy-based trust prediction model for routing in WSNs." *The Scientific World Journal* 2014: Hindawi Publishing Corporation Article ID 480202, <http://dx.doi.org/10.1155/2014/480202>, pp. 1-11.
- [39] Bisen, Dhananjay, and Sanjeev Sharma. "An enhanced performance through agent-based secure approach for mobile ad hoc networks." *International Journal of Electronics* 105.1 (2018): pp.116-136.
- [40] Abbas, Nihad I., Mustafa Ilkan, and Emre Ozen. "Fuzzy approach to improving route stability of the AODV routing protocol." *EURASIP Journal on Wireless Communications and Networking* 2015.1 (2015): 235, pp. 1-11.
- [41] GS Tomar, M Dixit, S Verma, "AODV routing protocol with selective flooding", International Conference of Soft Computing and Pattern Recognition, pp.682-686, 2009.
- [42] L Shrivastava, GS Tomar, SS Bhadauria, "Performance evaluation of reactive routing in mobile grid environment", International Journal of Grid and High Performance Computing (IJGHPC) Vol.3, No.3, pp. .2011
- [43] L Shrivastava, GS Tomar, SS Bhadoria, "A load-balancing approach for congestion adaptivity in MANET", International Conference on Computational Intelligence and Communication Networks, 2011.