Secured Intrusion Detection System Energy Routing Protocol for Mobile Ad-Hoc Network

Rajendra Prasad P., Shivashankar

Abstract: ***Mobile Ad-Hoc Network (MANET) works without any essentialsetupas required in the wired networks for its communication. Since MANETs lack a compact infrastructure type as its topology is dynamic, the major concern in this type of networks are the energy consumption in the routing and also they are prone to security issues in the networks as it lacks firewalls and sufficient software which fails to the data protection in wireless networks. To provide energy management and security to these networks types, many Intrusion Detection System (IDS) has been implemented earlier, that are focusing on either only the routing protocols or their efficiency, but they do not address the energy utilization and the security problems. In the proposed work, Secured Intrusion Detection System Energy Routing Protocol (SIDSERP) for mobile ad-hoc networks determines the best available route path, considering the energy utilization, also finds the alternate route path if the existing route path is malfunctioned, also provides the safety to the network by building an intrusion detection system. The proposed protocol work is carried out in network simulator-2 and comparison against the existing Ad-hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) protocols. The network performance metrics considered are the packet delivery ratio (PDR), throughput and energy consumption.***

Keywords: Energy, intrusion detection system, mobile ad hoc network, security.

I INTRODUCTION

Wireless networks and particularly mobile ad-hoc network are the future to all the devices for communication [1]. The MANETs operate without any sophisticated architecture built as in the wired infrastructure networks. These networks are able to connect any device at any given time in the network to communicate with each other.

This way of data communication processed by mobile users is not found in the traditional wired network, as the nodes are static or stationary in this type of network [2].

This process of communication enabling between the nodes for sending and receiving information to its associate co-operating nodes in the network, proposes the challenges on enterprise aspects of routing algorithms [2]. Generally, the routing protocols establish multiple links to route the data information in the networks and the routing proceeds between these nodes, only if data information is present to Forward. The objective of the routing protocols is to deliver this information to the nodes in the network [3].

In this type of networks, probable availability of multiple route paths form source to destination is offered, and the major critical issues is to determining the best available route path, considering the energy utilization, also alternate route path if the existing route path is malfunctioned due to the presence attacks, and provided that the safety to the ad-hoc network by introducing intrusion detection system.

The organization of manuscripts described as below, where the introduction of the MANET and design issues is provided in the Section I. The existing works in the MANETs contributes information about the available routing protocols, and secure intrusion detection system at the end of Section II. Routing protocols and the selection of the existing protocol are presented in Section III. Section IV gives the design and implementation of the research work,followed by the simulation of the SIDSERP work against the existing AODV and DSR algorithms in the Section IV. Conclusion of protocol and comparison analysis of the work, gives the analysis and shows increase in the performance with the existing protocols are described.

II EXISTING WORK

In demand to improve the existing routing protocols with energy managements and also providing the safety of the ad-hoc networks by introducing the Intrusion Detection System (IDS) in the existing protocols, it is important to build thesafety intrusion detection system that can compact with security issues in the network. Such security methods can be developed only with the extensive research on the existing protocols. The section is divided into two parts, where in the existing routing protocols with respect to the energy is discussed in the first part and the other section discussed about the secure intrusion detection system as described below.

A. Routing Protocols in Mobile Ad-hoc Network

Numerous systems in MANETs have been implemented and their impact on networks has been analyzed using different performance metrics. The major related design issues in mobile ad-hoc network are the route calculation. That deals to find the best and accurate route to sink node during the mobility and network topological changes and uniformly distributed. All these problems including reliable secured network and gaining accurate spectrum are considered in the earlier research work [4].

Revised Manuscript Received on December 15, 2019

Rajendra Prasad P.*, Assistant Professor, Department of Electronics & Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru and affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. Email: rajisvec@gmail.com

Shivashankar, Professor and Head, Department of Electronics & Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru and affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. Email: chenduss123@gmail.com

Researchers argue with a simple algorithm [5] providing implementation details that describes, and which provides connectivity of the nodes, and build the strong communication and the node limitation to the radio range in wireless communication. There are many protocols that are existing based on the shortest-path protocol mechanism and flooding algorithm is used in the proposed system. A dynamic routing algorithm is developed for possible elimination of the ideal links at the time of backbone network setup will not yield minimum energy solution for route calculation to establish and maintain the network for connection related sessions which make use of the knowledge of re-routing configuration to cope with the nondeterministic topology changes. The author [6] provides the shortest path routing algorithm used in MANETs in command to know the numeral nodes availablefor routing in the network.

For a wireless radio spectrum to communicate in a mobile network, the [7] provided that the MANETs differ significantly from other existing networks and co-operative network. The mobile nodes are dynamic in nature and also act as administration in the network topology. In [8] explained the nodes are self-configuring and intended to be de-centralized control in the network topology. In such networks, it is not desirable to assume all the nodes will have single hop communication with each other. So, such type of networks need specialized efficient routing protocols which provide self-starting behavior of mobility. In such situations, existing wired network routing protocols would degrades in performance. In wireless correspondence framework, there is dependably interest for new routing protocols have been on interest in MANETs. Invention of any new wireless routing protocol is categorizedbuilt on the mobility and character in which route data base consisting of the data tables are created, preserved and updation is done at regular interval.

For multi-hop communication various routing protocols have been proposed [8]. These protocols, traditionally evaluated in terms of data rate loss, packet overhead and route length. A growing emphasis on long-lived networks has added energy consumption as an important metric.

A number of research studies have been done on energy routing protocols of MANETs. Network performance based on energy has been major focusing area for research on routing protocols in MANETs. The designed conservative routing algorithms in which are performance based and optimization fairly energy efficiency is needed.

B. Secure Intrusion detection system

The secure IDS for MANETs are the other major concern that needs to be addressed. The security of the networks majorly depends on the cooperation provided by the nodes. The author [9] provided the intrusion detection system, where in the nodes cooperates is performed by the IDS agent in the ad-hoc network. These agents are liable for information forwarding/detection of any malfunction available in the network. The paper [10] presents the traditional way of intrusion detection layering structure where in the approach proposed the separating the routing and scheduling the energy of the nodes is described. But this approach is not appropriatefor ad-hoc wireless networks. The author [11] discussed the medium entree and direction-finding intrusion detection system is the building blocks of the wireless network.

The paper [12] explores the nodes features and discussed the routing variances when the IDS are considered for the MANETs. The author [13] presents an IDSprocess using a clustering protocol for the sensor networks. This paper discussed three types of routing attacks.

In [15], the authors provided the DSR protocolsfor the networks and provided the effects the performance metric. The analysis provided decrease in the PDR, throughput of the system. The authors provided different available algorithms in the network with high overhead.

The security of the network needs to be addresses by introducing the secure intrusion detection system that provides security to the network, along with the energy utilized routing protocols for the mobile ad-hoc network.

III ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORKS

Routing protocols in the MANETs are molded by sufficient size devices that can easily be accesses anywhere and anytime of the network. In the subsequent section, several available protocols based on routing will be discussed for the selection of the existing protocol suitable and present the novel proposed secured intrusion detection system energy routing protocol (SIDSERP) for the network.

A. Ad hoc On-demand Distance Vector Routing

The protocol finds its paths in the network by broadcasting a route request from the origin to all the associates nodes, till it reaches to the destination node. The route request process to all the associate nodes needs to provide the reply by the node by forwarding the route reply to the source from the destination node. The associate nodes update this information in the routing table and updated packets are again broadcast through the header packet in the network. This process is continuous till all communication is completed in the network. If network is malfunctioned with the link failure, then again the process should be started from the route request again.

B. Dynamic Source Routing (DSR)

This protocol is categorized into two phases. The initial phase is the route discovery and the other is route looking after phases termed as maintenance phase. The crucial difference between this protocol and other reactive protocols is the routing information is confined in the header packet of the protocol. As protocol sends the packet header to its associates, the nodes don't save the routing information in the cache memory. The associate's nodes can store this information to improve the network performance if required. Also the DSR protocols support the asymmetric links. DSR are best suited to the small networks consisting of 50-100 nodes.

C. Protocol Selection

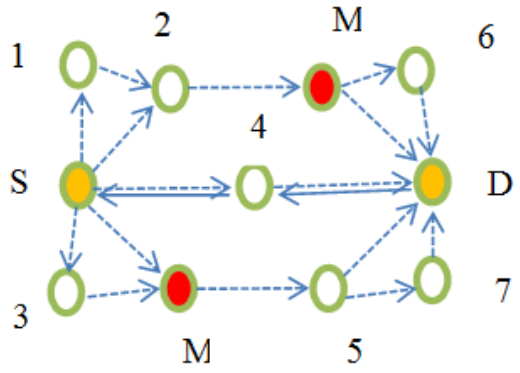
Out of all the routing protocols, i.e., AODV and the DSR protocol, the most scalable is the DSR because of its process of implementation and preferred for this manuscript as ease of enactment was one of the crucial selection aspects.

Both protocols procedure of transmitting information is different. In AODV the routing information is saved by the each node itself where as in DSR the routing information is included in the header packet. In comparison with the nodes mobility, the AODV performs better with less mobility and DSR performs better in high mobility in the network. Hence DSR was preferred,since it was the utmost efficient in terms of energy utilization.

IV SECURED INTRUSION DETECTION SYSTEM ENERGY ROUTING PROTOCOL FOR MOBILE AD-HOC NETWORK

Secured IDSrouting algorithm is proposed built on existing modified DSR algorithm for implementation of the SIDSERP. Energy factor is considered as main criterion for choosing a shortest route path. Diminish in the nodes remaining energy force expands the expense of a node. The goal is amplifying the lifetime of an ad hoc network. Basically to keep up the network topology information the nodes are not required for an on-demand routing protocol. Using a connection establishment process, the necessary path will be obtained by the nodes, as and when required. The stack wherein the diverse layer of the network protocol are focused in order to have better efficiency and different regressive practices have begun in the area of power conservation. On the other hand, the MAC layer and the network layer have been focused for the examination.

Consider a network model as shown in Figure 1 to understand the proposed secured intrusion detection system energy routing protocol for MANETs.



S = Source node, D = Destination node, M = Malicious Node

Fig. 1.A nework model

In the model presented, the source node {S} transmits the route request {RREP} packets to all its associates node, the nodes forward this route information till it reaches all the nodes in the network or till it extentsto destination node {D}.

The route paths from {S to D} in the network are provided as follows

Route 1 = {S-4-D},
Route 2 = {S-M-5-D},
Route 3 = {S-3-M-5-D},
Route 4 = {S- 2-M-D},
Route 5 = {S-1-2-M-D},
Route 6 = {S- 2-M-6-D},
Route 7 = {S- 2-M-5-7-D},

In the network two malicious nodes are present and the network implements the secure intrusion detection system in proposed protocol.

The flowchart of the secure intrusion detection system is shown in Figure 2.

Intrusion Detection System Module

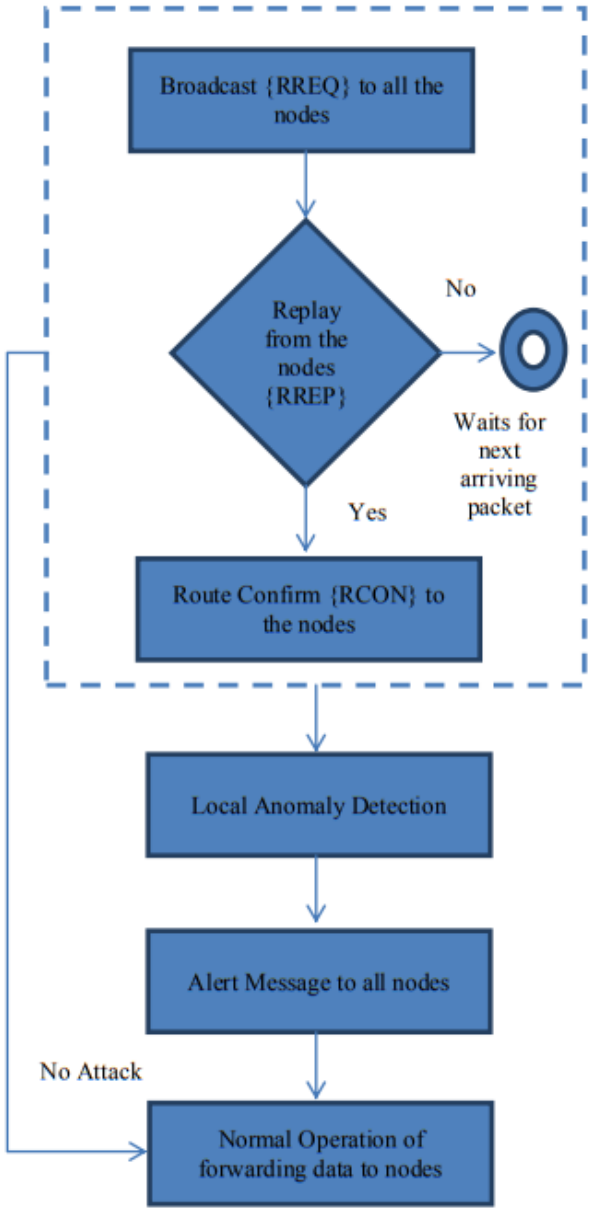


Fig. 2. Proposed IDS for MANET

In the proposed protocol, when the node receives messages/commands packets from its associates, the minimal energy required for forwarding packets to be active is denoted by (E_M) and the energy (E_L) is included to overcome the problem of unstable links due to channel fluctuations. The channel attenuation are calculated as difference of transmitted energy (E_{TM}) and the receiver energy (E_R).

The average energy consumption by nodes in network is computed by the equation (1) and it is generally measured in terms of Joules (J).

$$E_T = E_{TM} - E_R + E_M + E_L \quad (1)$$

The residual energy E_{RE} of the node can be computed by difference of the initial energy (E_I) with the consumed energy (E_C) in the network as given in the equation (2)

$$E_{RE} = E_I - E_C \quad (2)$$

Total energy average consumption of overall nodes (N) in network is given by the equation (3)

$$E_{Total} = N * E_I - E_{RE} \quad (3)$$

Secure intrusion detection system identifies the malicious nodes in network and sends alert messages packets to all the associate's nodes, thereby providing the security to the network and avoids malfunction in the network.

The minimal energy consumption and secure intrusion detection system applied to the network and the protocol finds the shortest route path as Route 1 {S-4-D}.

A. Energy saving Mechanisms

Wireless networks have to depend on convenient with limited energybattery. In communication, the energy consumption at the node energy is dominant when compared to the energy consumption in processing. Thus the communication system must have efficient energy to optimize the different states consumption communication.

Proposed network should satisfy both the security intrusion detection system and the minimum energy consumption to build the security intrusion detection system energy saving routing process for mobile ad-hoc networks. Thus secure communication, minimum energy between the nodes in the networks is implemented in the proposed work.

V EXPERIMENTAL RESULTS

Simulation of the proposed work SIDSERP with the existing AODV and DSR protocol respectively are implemented in the network simulator-2 considering the metrics packet delivery ratio, throughput with varying execution time and energy consumption with varying number of nodes respectively. The simulation parameters specifications are described in the Table 1 described below.

TABLE I: Parameter Specification

Simulator	Network Simulator-2 (Version 2.34)
Area	500m * 500m
No. of Nodes	100
Node deployment	Random way point
Transmission Range	200m
Initial Energy	100 Joules
Execution Time	200s
Traffic type	Constant Bit Rate
Communication system	MAC/IEEE 802.11G
Routing Protocols	AODV,DSR and SIDSERP

A.Performance Metrics

The parameters of the simulation are explained as below in terms of the packet delivery ratio, throughput and energy consumption.

$$PDR = \frac{\sum x}{\sum y} \quad (4)$$

where x is the total number of packets transmitted successfully that has reached to the destination and y is the total number of originated packets sent by the source.

In Figure 3, the PDRversus the execution time in termsof 50, 100, 150 and 200s respectively. The simulation results can be observed that the packet delivery ratio drops drastically with increasing execution time. It can be inferred that the AODV and DSRaffects the performance of the algorithm as compared to increased PDR in the SIDSERP.

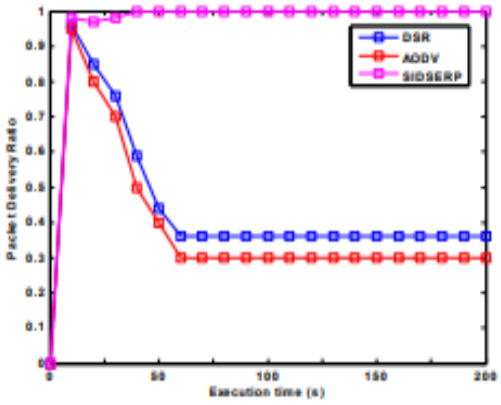
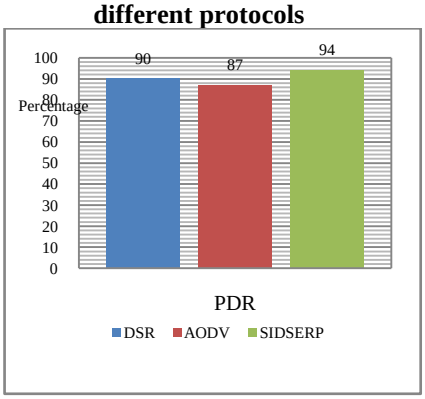


Fig. 3.Packet delivery ratio vs Execution time.

The Table II provides the PDR in terms of percentage for different protocols

Table II: Comparison of PDR in percentage with different protocols



Measure of data reaching successfully in the given period of time is termed as throughput of the network, and usually measured in kilobits per second (kbps).

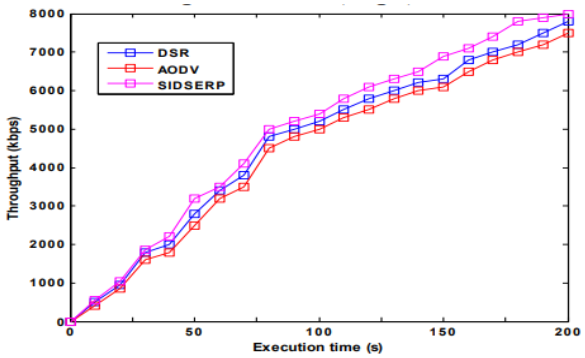
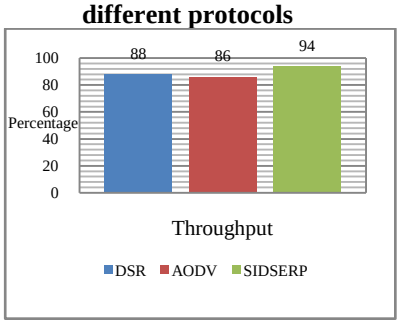


Fig. 4.Throughput vs Number of nodes.

Figure 4 of the SIDSERP, DSR and AODV protocol shows the variation in terms of the throughput. It is obvious that there is amazing decrease in the throughput.

Table III: Comparison of Throughput in percentage with different protocols



The Table III provides the throughput in terms of percentage for different protocols

Energy Consumption defined the average rate of the energy consumption of node times the time of operation.

In Figure 5, the energy consumption vs. the number of nodes is plotted. It is seen that the energy consumption increases with the number of malicious nodes.

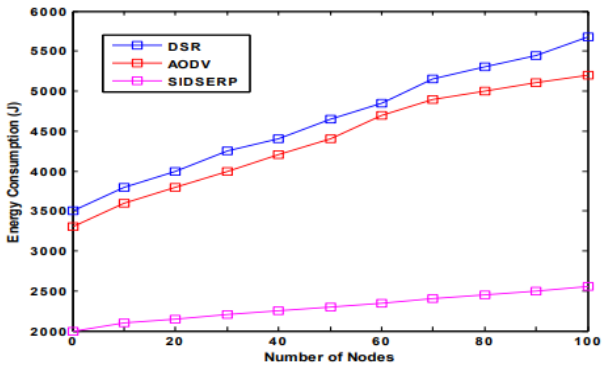
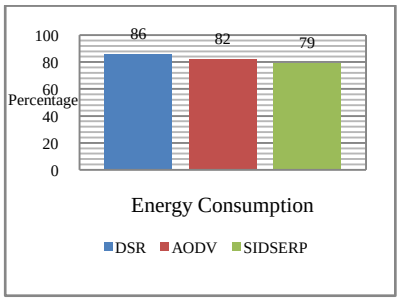


Fig. 5.Energy Consumption vs Number of nodes.

The protocol causes a significant increase in energy utilization. This adds to routing overhead leading to the massive increase in the energy consumption in the AODV and DSR protocol against the SIDSERP

Table III: Comparison of Energy Consumption in percentage with different protocols



The Table III provides the energy consumption in terms of percentage for different protocols

VI CONCLUSION

This paper presents a brief description secured intrusion detection system energy routing protocol. Energy is critical resource in the mobile nodes, so more efficient way of utilizing the energy is directly proportional to maximum network life time of nodes. The throughput and packet delivery ratio are also considered as major critical issues. Hence, it is difficult to design and develop a well-tailored ad hoc routing protocol by considering these parameters. Metrics such as minimum energy cost can enlarge the time till the first node goes down and hence the network partitioning time increases. Implementation is done with NS-2 simulator with scenario of 100 nodes. The observations are made with variation in execution speed in the network scenario. After analysis in different situations of network, it can be practical that SIDSERP perform better than AODV and DSR.The proposed SIDSERP enhances the performance increase in terms of its packet delivery ratio and throughput and decrease in its energy consumption as observed with the DSR and AODV protocol.

The future enhancement in this can be additionally built IDS in identification of the different kinds of attacks in the network and preventing.

ACKNOWLEDGMENT

We gratefully thank Sri Venkateshwara College of and Engineering, Bengaluru and Visvesvaraya Technological University, Jnana Sangama, Belagavi-590018.

REFERENCES

1. S. Olariu, Q. Xu, and A. Zomaya, “An Energy-Efficient Self-Organization Protocol for Wireless Sensor Networks”, Proc. IEEE Intelligent Sensors, Sensor Networks, and Information Processing Conf. (ISSNIP, pp. 55-60, Dec. 2014
2. Nazhad, SHH, Shojafar, M, Shamshirband, S, Conti, M, “An efficient routing protocol for the QoS support of large- scale MANETs”, Int J Commun Syst. 2018; 31:e3384. https://doi.org/10.1002/dac.3384
3. A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, “Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function” , IEEE Access, vol. 5, pp. 10369-10381, 2017.doi: 10.1109/ACCESS.2017.2707537
4. GRAWAL DP., MANJESHWAR A, “A protocol for enhanced efficiency in wireless sensor networks”, Proceeding of the 15th Parallel and Distributed Processing Symposium. San Francisco: IEEE Computer Society, 2015.
5. Sajal Sarkar, Raja Datta, “A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks”, Ad Hoc Networks, Volume 37, Part 2, 2016, Pages 209-227, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2015.08.020.
6. W. Kuo and S. Chu, “Energy Efficiency Optimization for Mobile Ad Hoc Networks”, IEEE Access, vol. 4, pp. 928-940, 2016. doi: 10.1109/ACCESS.2016.2538269
7. B. M. C. Silva, J. J. P. C. Rodrigues, N. Kumar and G. Han, “Cooperative Strategies for Challenged Networks and Applications: A Survey”, IEEE Systems Journal, vol. 11, no. 4, pp. 2749-2760, Dec. 2017. doi: 10.1109/JSYST.2015.2436927
8. S. Olariu, Q. Xu, and A. Zomaya, “An Energy-Efficient Self-Organization Protocol for Wireless Sensor Networks”, Proc. IEEE Intelligent Sensors, Sensor Networks, and Information Processing Conf. (ISSNIP, pp. 55-60, Dec. 2014
9. E. O. Ochola, L. F. Mejaele, M. M. Eloff, and J. A. van der Poll, “Manet reactive routing protocols node mobility variation effect in analysing the impact of black hole attack”, SAIEE Afr. Res. J., vol. 108, no. 2, pp. 80_92, Jun. 2017.
10. Eduardo F. Nakamura, Heitor S. Ramos, Leandro A. Villas, Andre. de Aquino, Antonio . Loureiro, “Reactive role assignment for data routing in event-based wireless sensor networks”, Computer Networks, March 2017.
11. Senol Zafer Erdogan and Selim Bayrakli, “Genetic Algorithm Based Energy Efficient Clusters (GABEEC) in Wireless Sensor Networks”, Procedia Computer Science 10, 2015.

12. S. Hamalainen, H. Sanneck, and C. Sartori, ,“LTE self-organizing networks (SON): network management automation for operational efficiency”, John Wiley & Sons, 2015.
13. S Shankar, G Varaprasad, HN Suresh. "Importance of on-demand modified power-aware dynamic source routing protocol in mobile ad-hoc networks", Microwaves, Antennas & Propagation, IET 8 (7), pp. 459-464, 2014.
14. H. Moudni, M. Er-Rouidi, H. Mouncif and B. El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks," 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV), Beni Mellal, 2016, pp. 385-389.
15. Rajendra Prasad P, Shivashankar, “Improvement of Battery Lifetime of Mobility Devices using Efficient Routing Algorithm”, Asian Journal of Engineering Technology and Applications, [S.l.], pp. 13-20, 2017.

AUTHORS PROFILE

Rajendra Prasad P. was born in India, in 1986. He received the B.E and M-Tech degree from Visvesvaraya Technological University, Jnana Sangama, Belagavi in 2008 and 2010 respectively and now pursuing the Ph.D in the wireless communication in Visvesvaraya Technological University, Jnana Sangama, Belagavi. Since 2011, he has working as an Assistant Professor in the Department of Electronics & Communication Engineering at Sri Venkateshwara College of Engineering, Bengaluru. He is the author of the several articles published in International/National Journals and conferences. His current interest includes wireless network, communication, mobile ad-hoc networks, security. He is also a reviewer for several journals and conferences.

Shivashankar was born in India, in 1979. He received the Ph.D degree from Visvesvaraya Technological University, Jnana Sangama, Belagavi in 2014. His Specialization is wireless communication and his research interest includes Focus on Wireless Ad Hoc & Sensor Networks and Cognitive Radio with emphasis on Design & Analysis of MAC and Routing Protocols. Cross Layer Design and Cooperative Diversity Schemes to Design & Analysis of MAC and Routing Protocols. He has received DST/AICTE/VGST/KSCST project funds. He is also the EXECOM MEMBER IEEE COMPUTER SOCIETY. His research publication includes in the reputed journal/transaction and conferences. Presently working as Professor and Head, in Department of Electronics & Communication Engineering, Sri Venkateshwara College of Engineering, Bengaluru