International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 12 ǁ 2021 ǁ PP. 26-33

Efficient Peer to Peer Routing Technique (EPPR) Model to Protect WSN from DoS Attack to Enhancing Wireless Communication Performance

Simran Khan
M. Tech. Scholar, All Saints' College of Technology, Bhopal, India

Sarwesh Site
Professor, Dept. of CSE, All Saints' College of Technology, Bhopal, India

ABSTRACT*: We know very well that a wireless network contains multiple small nodes called stations whichhave the capacity to process communication through sensors, access stations and workstation Services. Since WSN is growing in day to day business, at the same time, users and applications are also gets higher and higher since WSN support mobility services at run time, so that form along time many researchers and scientist has doing their work in WSN, in order to improve WSN communication services and to be reduces the security issues but still there are multiple serious measure need to be comes into the solution so that It could be improve as much as possible. Through various literatures we find various challenging issues in WSN along with attack issues which is need to be resolve as safety reason.*

Network users are easily accepting the services of WSN network hence users are growing day to day one need to improve the services of WSN so that it should be reliable as possible and people can faith on it, in order to protect wireless sensor network from multiple miscellaneous attacks and errors count during routing process so many research are going on along with more secure and strong security algorithm, like similarly this research also concentrate on the drawback analyzed by author to protect routing efficiency at physical and data link layers, in this paper we proposed an Efficient Peer To PEER Routing (EPPR) model that works on the concept of shield node framework to provide an effective and attacks free environment in order to authenticate original sensor node and intruder nodes.

KEYWORDS*: WSN, Dos Attack, Routing, key management, NS2, PDR*

Date of Submission: 12-12-2021 Date of acceptance: 26-12-2021

I. INTRODUCTION

Now are days Wireless Sensor Network (WSN) is the mostly used in real time communicationenvironment framework which specially designed for on demand user services which does manychallenges in front of its developers such services are commercial and real times basedapplications, its users are growing because of its user friendly simple procedural developmentenvironment via different workstation, these application are main aim to provide most secure communication system which likely to be useful in military purpose or measure all the differentfactors of weather and its forecasting since sensor based network is free from networkinfrastructure based complexity there for it is easy to install and isolate problem in WSN at thesame time extension based on demand can be manage at any time use standards servicesspecifications. WSN based network also very useful for the different purpose or objectives.

Wireless Sensor networks (WSNs) communicate through the process called rely on for the purpose of message exchanging and interaction among the network nodes, WSN support distributed frequency channels to get successful completion of Request and Reply data delivery services during this operation many time attacks get occurred and it does heavy loss of data and many times it is responsible for link failure and server hacking activities.
In this paper we concentrate on the services of DSR and SAODV protocols since wireless routing play an important role for the management of security and privacy during routing operations. The forwarding phase of routing is easily handled by SAODV protocol but in the last phase of packets delivery it suffers from delay factors as well as sometimes it gets loss data as well [1], even when SAODV uses highly encrypted data processing instructions. On the other hand other protocols like RAEED-EA is the latest invented protocol of WSN which aiming to

makes nodes more efficient in working as well as to provide a way to successfully complete the routing process along with all the phases here security has been majored and reliability has becomes the big advantages over the design of RAEED-EA protocol in WSN , but sometimes we found as the traffic pattern varies RAEED-EA gets down its performance level with inconsistency , we analyses the working of this protocols it is not good for the condition of DoS attack situation , attacker can easily break the services environment using fake nodes so that it is still a big challenge for computer researchers to design a new framework that can manage performance with higher no of nodes and also applicable to identify fake node so this survey study brings WSN challenges to overcome the weakness of traditional routing protocols and to improve WSN under dos attack[2 ,3].

It is a matter for research to protect our network from the effect of congestion in wireless network, to overcome from this issues there are many researches has proposed and continuously working on them to make network error free as possible. In[4], author proposed Proportional Integral Derivative Model for resolve peer to peer network error control arises at fluid algorithm in wireless distributed network, in the proposed design one experimenting primal dual method in order to improve performance at throughput level rather than stability , algorithm has PID frame that takes the responsibility for performing controlled action along with distributed design scenario, it is good at some extent level but simulation study define variation at performance level has been introduced as traffic get heavy. Static Load Balancing can be effective solution based on topological aspect describe in [5] to define traffic engineering that focus on the capacity of link at run time dynamic to control and manage the load, the aim was to represent MPLS application to manage load, here one define when algorithm found in shortest path in Wireless Sensor Network then protocols instruction takes the role to get select low load shortest path instead of previous one, based on the bandwidth optimization and computation .congestion in Wireless Sensor Network can be the stronger barrier for wireless and wired communication if one talk about 3g void communication technology like in[3], network offer high speed data transfer but still there is many issues are happing at the time of communication due to heavier load of data to resolve these issues author proposed new design that expanding the network with parameter support. In[4], Genetic algorithm has been introduced for balance load at link level it can the solution for peer to peer network in modern network that manage non directed distributed traffic , experiment show it can be the better solution than other even it can be implemented at higher traffic area. Next hop routing is very common in routing algorithm to choose best interface among all. This techniques is dealing with big risk of getting failure of network , provides loss of information, in[5,6] one present a routing protocols named as multi next hop routing information protocol, the proposed techniques is the extension of RIP technique. As discussed there are many reasons, in network that responsible to carry the side effects during the communication that causes variation in throughput and data loss error, apart from above discussion few more side effect is measured as following.

- Availability, many times user experience blocking in this case redialing is performedmultiple Users are getting higher in number for the multiple services provided by the networkand the supporting infrastructure that convince large number of user to get network services.
- Due to limited path times causes side effect to networkstatus.
- Wireless network technology consist device portability function therefore network load is getting higher and higher.
- Run time subscribes are takes an important consideration to deal with connectivity error in which market policy for network users and pricing schemes affect the scenario of one time network subscriber.[7]
- Telephonic network provide great deal with existing and new network infrastructure to manage network overheads and maintenance due to this reasons users are getting higher and use network channels for multiple application , as result production of data is large it may causes network is affect from connection error [8-10].

WSN is a very challenging area of networking, many researchers is working on the problem Statements, in this paper we try to achieve following objectives.

- Proposed EPPR model will focus on the errors raised at physical and Data link layer during communication like to avoid DoS Attack to maintain the performance and reliability of WSN.
- To provides node authentication and verification to avoid node tempering attack
- Proposed model provide a protection layer of shield nodes, who detect fake node as well as authenticated nodes to provide WSN resource services without any interruption.

- Proposed Model also improves the Throughput, End to End delay and Packet delivery ratio services.

Organization of paper consists of 5 sections. In section 1, we introduce to WSN technology about its working, challenges, architecture and Attacks with proposed objectives. It is always necessary to have some challenges and motivation so that we can do our research in correct direction and right method need to be implement. Section 2 Literature Survey discuss the problem area of WSN and Attacks who introduces in network using different way, to define such things author go through different literatures form different reliable sources like IEEE, Springer and ACM libraries also referred from some good journals of computer sciences. Section 3 define proposed method, proposed algorithm and flow chart.

Section 4 explain the implementation detail of proposed model over NS2 networksimulation since NS2 support TCL language compiler so that it is good and supportive fordynamic networking environment, therefore we decided to perform the implementation onNS2. This section also defines the graphical comparative study between SAODV, RAEEDEA, and EPPR for throughput, end to end delay and packet delivery ratio along withConclusion and Future Scope.

II. RELATED WORK

In [11] author present a unique approach to control over the problem of congestion in ―Link Congestion Control Mechanism Based on Multi Topology here author„s are resolving the major reasons of the occurrence of congestion in network, that is (i) Due to the Lack of resources.(ii) Irrelevant use of available network recourses i.e. resource position like router position to get manage data and distributed traffic to reduce complexity at network level.

In [12] presents a novel approach for dynamic congestion control mechanism for real time streams over RTP , this research presents the mechanism to handle growing network due to the high demand and production of multimedia applications, author suppose the problem due to the massive growth in multimedia oriented application which uses data in the form of streaming like audio, video, etc such application produces large amount of data continuously causes stress over network that result, bottleneck problem on link due to heavy congested network , to address the solution regarding the bottleneck link author proposed a reliable, dynamic congestion control .

In [13] author presents mechanism for wireless network belong to the services category of protocol IEEE 802.11 wide area network. Author design a novel point to point connection oriented congestion control mechanism known as ―Media access congestion control ― the major object behind this research is to control on fluctuate rate of sender and receiver window . MACC improve the performance by having control over sending rate. so that synchronized communication can be achieve to get successful communication in wide area network ,such congestion control has been done at MAC layer to get reduce flow error occur due to congestion, MACC is useful to utilize channel capacity effectively and also capable to manage fairness at both end. Proposed model has been design after the analytical study of wired and wireless communication architecture regarding the study of congestion. In order to eliminate congestion from wireless local area network author mainly focus on the experimental study of congestion at wireless network on WSN reliable congestion less protocol. Another important research to control congestion error has been performed by author.

In [14] proposed new mechanism to improve efficiency in network ―Exploring the Scope of Infinite-Band congestion control mechanism that describes new mechanism in the form of Infinitebased congestion control technique , here researcher's is working on the concept of fair distribution of network and required allocation of available resources so that one can have loss less connected efficient network , author focused on the detection and solution of congestion on time problem can be manage with right action , if countermeasures taken afterward it causes growth in the form of congestion tree that affects contribution for the high congestion . If one left such thing at primary stage then tree will grow and block traffic flow that lead drop network performance.

In this literature one present solution for two measure factor of discussion whenever one talk about the WSN Error, it has been always a questioned that Mechanism is capable to manage traffic at run time and if what happen? if traffic is flowing with different network parameter so is it capable to manage and change parameter accordingly, requirement of parameter is different in the form of patterns as the use of application in network. Experimental study show that mechanism are sufficient enough to get dynamically increasing and growing the set of parameter values as per the need with the maintaining network performance level on every outgoing network traffic load [15].

In [16], presents mechanism for wireless network belong to the services category of protocol IEEE 802.11 wide area network. Author design a novel point to point connection oriented WSN Error control mechanism known as ―Media access WSN Error control ― the major object behind this research is to control on fluctuate rate of sender and receiver window

In[17] design a attack detection technique in WSN with different level of traffic pattern and multiple variation in sensor based network , the major object of paper was to provides as attack detection technique and utilize energy level of nodes. In [18] another routing based sensor network protection scheme has been proposed in this paper along with review report and analysis of different errors and effects of attacks over WSN , in this paper author concentrate to resolve jamming attack during WSN operations and fluctuation among the sensor nodes and detection of jamming error throughout the routing process along with the observation of sensor nodes moving into WSN communication ranges with different level of energy consumption , at the end of the paper author present an forecasting report based on the future challenges and complexity rises of WSN since wireless network user as growing and presenting different challenges in day to day business operations.

In [19] author define the effect of DoS attack on different layer of network over different protocols, the story of DoS represent from the first non authorized node which can affect the network services from application level and such fake nodes gets and perform the multiples for the initial server in order to get engage the overall capacity of main server using such dummy sensor nodes.

III. PROPOSED METHDOLOGY

Now are days WSN network is the best for real time current application like simple type of network communication based processes for military applications, health monitoring based real time operation etc In such application WSN network signals is widely used for the management of battle signal inflations, to search and observation of biological based communication and to investigate regarding different types of chemical viruses and attack. In health application environment it is compulsory to observe patient investigation time to time which can handle through such model so that it is easy to get locate doctors tracking and communicating the actual report with associate doctors to resolve complex situations.

To resolve the complexity issues occurred in WSN routing we has proposed a new scheme or model that will overcome on the discussed issues as much s possible which has been doing wellwork along with WSN specification and environment called ERR model in this we major focused on DoS attack in WSN, it avoid hello food attack and manage the performance factors during the network protocol services and communication system.

Proposed Method

ERR resolve the issues using shield node techniques to immune the network from DoS attack as well as from Hello Flood Attack . Our proposed method will follow following phases during process in WSN:

- Key Management Setup
- Routing Process Setup
- Key Exchange Setup

As shown in figure 1 we can say that here sensor node has n number of neighbor it may possible that among such node any node can be an attacker nodes as we can seen in figure 1 ,here when every node received ACK message , every node will provide an assign message back to the source node aw part from the other unknown node it may be attacker node here we propose an new thing in which to avoid the attacker node to be get contacted through the network we will detached the communication links to protect our network from DoS attack.

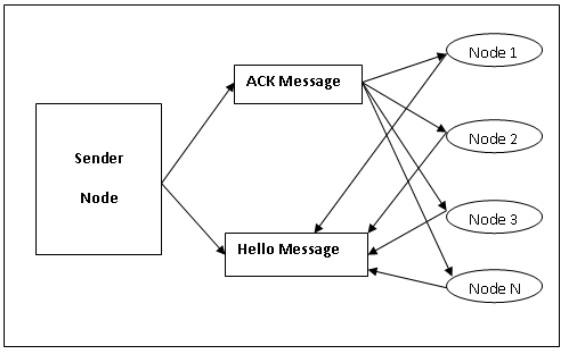

Figure 1: Process of Key Exchange Setup in WSN

Proposed algorithm

In sensor based network, communication may take pace an important part when all the shield based sensor node get interact to each other where ever active shield station needs send identified data or information to other intermediate base station , during this process many time there is a chance of finding some other specific nodes that may be an intruder or else it can be the part of straightforward active zoon of origin server or other participated nodes in this case we use algorithm 1 to take the responsibility of finding such sensor node for the elimination of attack free WSN network.

Algorithm:

- First of all one need to initialize all the shield nodes along with their initial values and timer should set with T1 time parameter.
- At time T1 Shield node server synchronies all the available authorized nodes that play their role for accessing the server, through this server establish an active nodes session for their specific ranges of data transmission using sensor nodes.
- To capture routing scenario efficiency we introduces the fake intruders node with shield node at time T1 so that one can measure the avoidance of such intruders nodes and test the performance and security level of proposed scheme under DoS attack situation.
- During routing process cache has been manage for maintaining all the incoming and outgoing process at time T1.
- Shield nodes have been verifies through authentication process via server.
- Server place all the verifies shield nodes in active session and remaining nodes into passive session so that all the not verified nodes can be avoid to participate during data transmission .
- To detect DoS attack during accessing server should follow the EPPR policy and check weather available connection limit exceeds , if yes it should reject connections since it may an intruder node or DoS attack client

- Similarly during process one also check the bandwidth measurement since through this one can identify the attacks as well, so if nodes cross its bandwidth limit, if yes then again, connection should be rejected otherwise connection accepted and data transmission proceeds.

- Process routing to receive server response for successful completion of process.
- At the end measure the result with Throughput, End to end delay between nodes and measurement of packet delivery ratio using ns2 xgraph tool.

Flow Control Chart of Proposed Model

In the process of avoid the situation of DoS attack and the purpose to sole the attack issues so that in advance we can detect such suspicious node during the process so that we can identify the capacity of our origin server and the required bandwidth distribution among the sensor node using buffer optimization process so that relay can be gather throughout the process of sending and receiving data using shield sensor node. The Flow chart of proposed model shown in figure 2

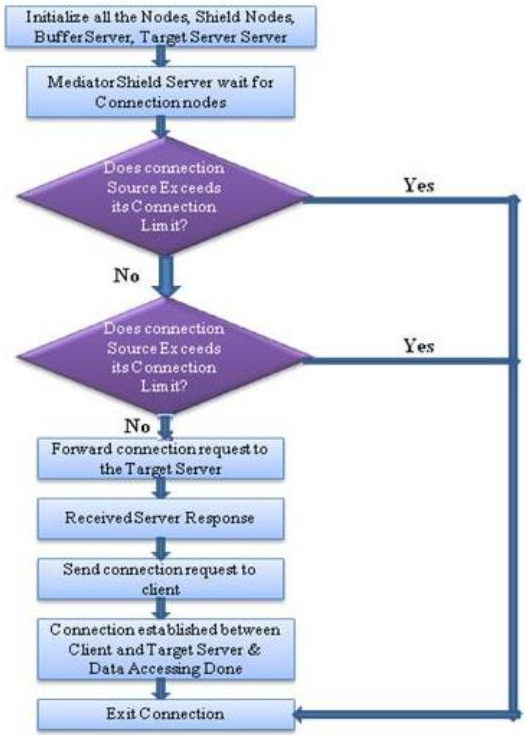

Figure 2: Flow chart of proposed model

IV. RESULT ANALYSIS

In this section we simulate and perform series of experiments with varying numbers of sensor nodes with different traffic intervals, all the nodes has been associate with the simulation area of 1000×1000m. Random walk has been generated with CBR over source and destination, to get simulates the series of experiments for comparison of result.

The NS2 Simulator is dedicated to the discrete time variant frequency analysis time-oriented testing system, in NS2 we can simulate program using C++ object oriented and oriented tool command language are utilize to perform random experiments in which comparison can done using X-graph tool to get compare the result and proof the changes made in algorithm

To determine systems nature, we compute PDR so that system fluctuation can be major at run time processing environment, it also defines the overall framework of the system. Following majors and parameters has been carried out using Packet Delivery Ratio.

PDR=Number of Packet Delivered/Time (1)

In following figure 3 we can discuss the Packet Delivery Ratio under DOS attack condition , in which practical implementation of proposed code demonstrate the result of ERR algorithm in superior way.

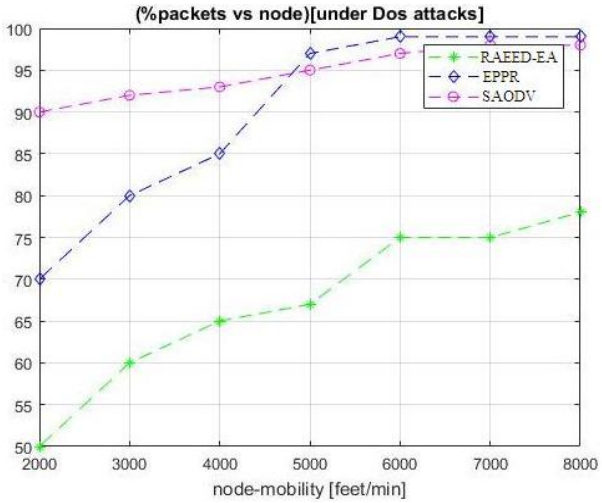

Figure 3: Packet Delivery vs loss ratio under Dos Attack

On the other hand in figure 4 demonstrate that total time took by the sender node to transmit the data efficiently to the desired destination it has been compute and majored in network term called End to End Delay consideration using following equation we perform End to End delay.

End To End Delay=Packet Arrival Time-Packets sent Time/Number of Connection (2)

Figure 4 demonstrate the resulting parameters of proposed model for End to End delay , here we graphical analysis defines that proposed scheme maintain manage with tolerated End to End Delay in WSN

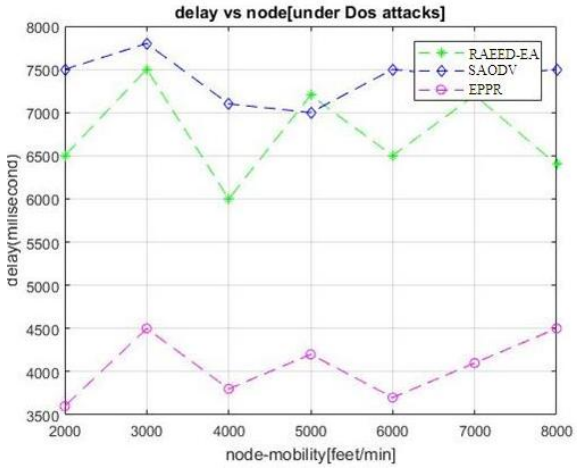

Figure 4: End to End Delay under Dos Attack

Whereas throughput is another important variant to be discussed in figure 5 which describes that total amount of Data Packets need to be sent to the desired destination in specific per unit of time. In our approach throughput measurement and computation has been done using following formula:

Throughput =Number of Packets Delivered/ Time Period (3)

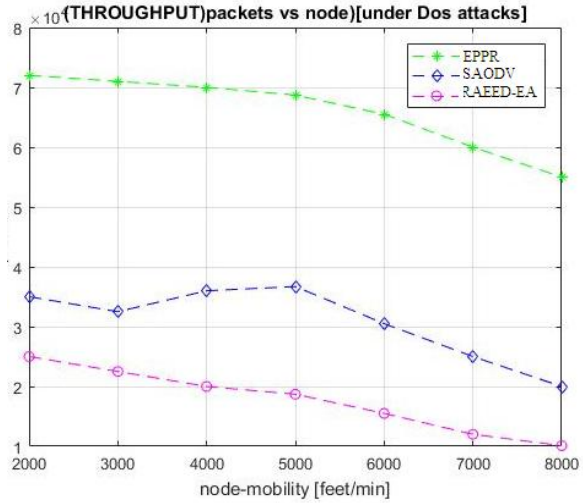

Figure 5: Throughput under Dos Attack

V. CONCLUSION

In this paper proposed secure ERR scheme perform well under DoSattack condition with different traffic pattern and values, our proposed scheme answers for different attack in study with NS2 simulation. The used scheme utilize the bidirectional Omniantenna phase with check point technique from distance for transmission of data packets againstHello Message attack and Flood Attacks, it defines safe and secure communication, verificationand also maintain authorization of nodes

under attack possibility, using this scheme we got verygood results for the point of view of performance, efficient and security in under DoS attackcondition.

In future we need to proposed more reliable and trustful solution for the improvement of quality of services in WSN, since in near future WSN application are growing we need to focus on more secure and authentic communication services .

REFERENCES

[1]. S.Umamaheswari, N.S.Usha, E.A.Mary Anita, K.Ramaya Devi, Published paper titledas "A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN" in IEEEInternational Conference On Information Communication And Embedded System(ICICES 2016), DOI No. 978-1-5090-2552-7.

[2]. Halawani, S., Khan, A., Sensors Lifetime Enhancement Techniques in Wireless Sensor Networks - A Survey Journal of Computing, vol. 2, issue 5, May 2010.

[3]. Bachir, A., Dohler, M., Watteyne, T., Leung, K., MAC Essentials for Wireless Sensor Networks. Communications Surveys & Tutorials, IEEE. Vol. 12, issue2, 2012 pp. 222- 248.

[4]. Y. Yan, Y. Qian, H. Sharif, and D. Tipper, ``A survey on smart grid communication infrastructures: Motivations, requirements and challenges," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 5_20,1st Quart., 2013.

[5]. Hui Jiang Energy big data: A survey, IEEE Journal and Magzine, vol. 4, 2016, pp 3844- 3861 DOI: 0.1109/ACCESS.2016.2580581

[6]. Adam B. published "Structural Health Monitoring Using Wireless Sensor Networks: A Comprehensive Survey in IEEE Communications Surveys & Tutorials, VOL. 19, NO. 3, Third Quarter 2017.

[7]. Muhammad Asifl, Shafiullah Khan," Quality of Service of Routing Protocols in Wireless Sensor Networks: A Review" vol. 5, 2017, pp 1846-1871, DOI: 10.1109/ACCESS.2017.2654356.

[8]. Sunil Kumar Singh," A Survey On Successors Of Leach Protocol" IEEE Access vol. 5, 2017, pp 4298-4328,DOI: 10.1109/ACCESS.2017.2666082. 55

[9]. Victoria J. Hodge," Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey" IEEE Transactions on Intelligent Transportation Systems, Vol. 16, No. 3, June 2015.

[10]. Hlabishi I. Kobo," A Survey On Software-Defined Wireless Sensor Networks: Challenges And Design Requirements" vol. 5, 2017, pp 1872-1899, DOI: 10.1109/ACCESS.2017.2666200.

[11]. HoudaMoudni, Mohamed Er-rouidi et al., "Performance analysis of AODV routing protocol in MANET under theinfluence of routing attacks" In Proceedings of IEEE International Conference on Electrical and Information Technologies (ICEIT), 2016, 4-7 May 2016.

[12]. T.R. Andel et al., Automated evaluation of secure route discovery in MANET protocols, pp 26–41. Springer, 2016.

[13]. Y. Hanna, et al., A domain-specific verification framework for sensor network security protocol implementations. In Proceedings of the first ACM conference on Wireless network security, Alexandria, VA, USA, pp 109–118, 2016.

[14]. K. Saghar, W. Henderson, D. Kendall, and A. Bouridane. Applying formal modelling to detect DoS attacks in wireless medium. In IEEE, IET International Symposium on Communication Systems, Networks And Digital Signal Processing Nasa/Esa (Csndsp 2018), 2018.

[15]. D. Cazorla, et al., Model checking wireless sensor network security protocols: Tinysecleap. In Proceedings of the First IFIP International Conference on Wireless Sensor and Actor Networks (WSAN"15), pages 95–106. IFIP Main Series, Springer, 2015.

[16]. C Siva Rama, C. Murthy, B.S Manoj, Ad-hoc Wireless Networks Architectures and Protocols, Low price Edition, Pearson Education, 2017.

[17]. D. Kumar, A. Srivastava, and S. C. Gupta, "Routing in Adhoc Networks under Reference Point Group Mobility," European Modelling Symposium, IEEE Computer Society, pp. 595-598, 2013.

[18]. A. Agarwal, S. Gandhi and N. Chaubey, "Performance Analysis of AODV, DSDV, and DSR in MANETs," International Journal of Distributed and Parallel Systems (IJDPS), Vol. 2, No.6, November 2017, pp:167-177.

[19]. S. Gandhi, N. Chaubey, P. Shah, and M. Sadhwani, "Performance evaluation of DSR, OLSR and ZRP protocols in MANETs," Computer Communication and Informatics (ICCCI), 2012 International Conference on, pp. 1-5, 2012 protocol. In NASA/ESA Conference on Adaptive Hardware and Systems (AHS- 2010), 2017.