# An Investigation on Peer To Peer Network under Network Attack (DoS)

**Praveen Kumar Mohane[1] Dr. Ravi Verma[2] Prof. Chetan Agrawal[3]**
[1]M.Tech Scholar [2]Associate Professor [3]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]Radharaman Institute of Technology & Science, Bhopal, India

*Abstract*— Now are days Wireless Sensor Network (WSN) is the mostly used in real time communication environment framework which specially designed for on demand user services which does many challenges in front of its developers such services are commercial and real times based applications, its users are growing because of its user friendly simple procedural development environment 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 different factors of weather and its forecasting since sensor based network is free from network infrastructure based complexity there for it is easy to install and isolate problem in WSN at the same time extension based on demand can be manage at any time use standards services specifications. 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 so that we are going to present an survey study of peer to peer network under network attack.
***Key words:*** Peer to Peer Sensor Network, WSN, Network Attacks, DoS Attack, Black Hole Attack

## I. INTRODUCTION

A Local Area Network like Wireless dynamic network is a collection of distributed networking components and networking resources will be engaged to process some task mobile users communicating via a wireless station. The node can be any device such as a PDA, laptop etc. will be used for connectivity mediator. Such networks are usually considered as intranet area networking services used for office work regarding data communication, and are most prevalently used in many offices nowadays. We can classify it in 3 types of WLANs – Independent Basic Service Set, Basic Service Set also referred in mobile communication, Extended Service Set. IEEE 802.11 is primary used for WLAN services is an adopted international standard for LANs which support data transmission capacity from 1 Mbps to 58 Mbps in either the 2.6 GHz or 8 GHz frequency channels. The latest version used today is IEEE 802.11g which provides a high bandwidth compare to previous one that is like of up to 54 Mbps. Following figure 1.1 illustrate the type of network which we discussed earlier.

Wireless Personal Area Network is a collection of personal distributed sharing devices which communicate without any dependability on underlying networking framework. The Ethernet IEEE 802.15.1 standard used for WPAN network, also called like an example which we called popularly as the Bluetooth is now are days used for short range high capacity communication via signaling system coordinated and supported by various wireless devices like digital cameras, PDAs, laptops, etc.

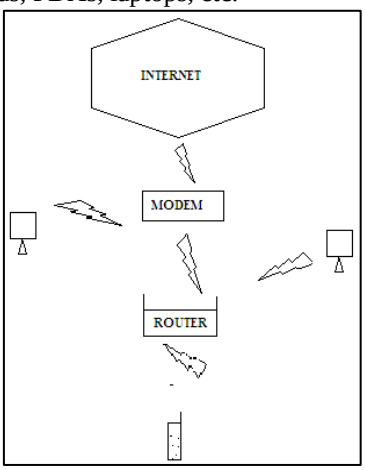


Fig. 1: Example of WLAN

Now are days Wireless WAN and MAN network has been concerned with allocation of computing network resources where multiple node are participating in different way to each other as in figure 1.2 In order to process the wireless data transfer services and the protocol services for the best of safe data transmission along with the best performance state to make network more effective [5] , if one talked about WLAN they need to go through the deep study of available network resources as well as the role of different node and resources along with the oberservation of traffic issue and congestion problem , in case of high traffic level many times load of congestion get higher since available resources and their capacity gets lower compare to the required one. In this case we need to design a kind of network that can handle the node and data load and perform as expected with the introduction of some buffer management and optimization based technique [6].

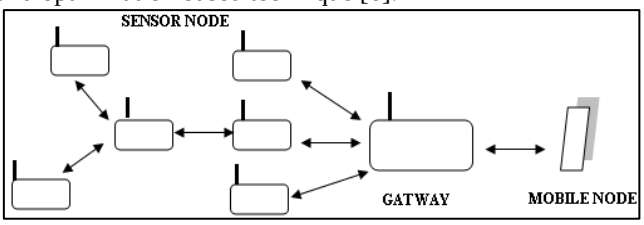


Fig. 1.2: Example of WSN based Communication System

## II. LITERATURE SURVEY

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[1], 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 [2] 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] one present a routing protocols named as multi next hop routing information protocol, the proposed techniques is the extension of RIP technique.

Another important research to control WSN Error has been performed by Gran in [6] proposed new mechanism to improve efficiency in network ―Exploring the Scope of Infini-Band WSN Error control mechanism‖ that describes new mechanism in the form of Infini-based WSN Error 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 WSN Error on time problem can be manage with right action , if countermeasures taken afterward it causes growth in the form of WSN Error tree that affects contribution for the high WSN Error . If one left such thing at primary stage then tree will grow and block traffic flow that lead drop network performance. Proposed WSN Error control mechanism resolve the WSN Error affect before the growth of WSN Error tree so that it could not be able to hamper the performance of network slowdown, mechanism consist rich set of parameters that produce effective WSN Error control and cooperative network for high throughput and it is fast enough to manage dynamic network traffic load based on demand base

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 [7].

QoS is one of the major issue ever one talk about the reliable and efficient services because services for voice and data is compulsory to follow the aspect covered in the term like QoS that supposed to get many things like reliability, security, confidentiality, integrity and manageability during the complete flow of communication, that provides WSN Error less network communication architecture discussed. Many mechanism has been proposed previously they discussed service to improve best effort flows but all are not sufficient and suitable for the point of view of quality of service requirements , proposed scheme provides such quality of services with the help of equation based mathematical construct to get WSN Error control for different network working scenario, algorithm support WSN Error control mechanism with QoS service architecture , method consist functions like data loss control at router end , WSN Error control at sender and receiver end [8].

In [9] proposed a new WSN Error control mechanism with adaptive WSN Error window, designed to improve the performance of traditional WSN Reno cause problem during decline of connection protocol due to the over flow of bottleneck link buffer affect the performance of overall algorithm used for the increasing traffic scenario. Proposed network scheme define a modified in already defined WSN algorithm based on the distribution of available link capacity, such capacity has been distributed in some intelligent share propositions. Proposed ideal analyze the limitation of traditional WSN protocol and define new WSN mechanism called as ABE_WSN which has the ability to dynamically manage the WSN Error window at run time for wireless networking environment that works on the calculation of available bandwidth. Proposed algorithm getting decision to adjust WSN Error window on run time and adjust the slow start threshold dynamically with the help of parameter adjustment and setting scenario that result the degree of packet loss due to overflow error is getting less and increases performance effectively.

As the extended version of recently discussed model ABE_WSN has the limit to manage network according to the single window capacity design that get cause a problem for high scale network, as the network spacing getting threshold down accordingly, result low performance congested network, to get it improve significantly, In [5] brings a novel mechanism to get more efficient functioning that consist double WSN Error window instead of single one like ABE_WSN. Author of the research get the title as ―An overview of packet reordering in transmission control protocol (WSN): problems, solutions, and challenges ‖ describes fact that wireless network follows many extra functioning rather than wired network which make traditional approach not suitable for wireless environment such novel model is known as DW-WSN . As one knows that users can be increase and decreases at any time in wireless portable network scenario sending window rate should be in control so that unnecessary corruption can be avoided that lead to higher reliability and serve as a energy sever for limited size

 

mobile devices DW-WSN resolve the WSN Error problem by define the solution in two way like one window handle disposing functions for WSN Error window and another handles disposing of error code window. The presented mechanism provide high reliability factor in wireless communication network by just getting a small variation in throughput rate and sending window threshold rate.

In [10] proposed an impressive WSN Error less network management technique, in that it describes an important consideration regarding the management of network in harmful WSN Errors environment research has been proposed with the title as ―TMRCC: A WSN Error Control Mechanism for tree based many to many multicast reliable multicast protocols ‖ in which it get the value to the key task as WSN Error control over the aspect of reliability when someone talk about the multicast networking scenario with error and flow control mechanism , there are so many mechanism has been already proposed as MWSN and TRAM are specially there for one to many multicasting but suffer with some limitation and drawback when network relationship comes from one to one to one to many , that why such mechanism has Bering some more special functioning to eliminate the indentified drawback from the previous model of WSN Error control , it working of the concept of WSN Error windowing technique with the measurement of rate controller is used in addition , feedback message is design to reduce the overhead at receiver site so that WSN Error has been reduces at some extent , two timer is used to manage positive and negative Acknowledgements ,such frame is used to reflect the position of dynamic network activities. To get load distribution quickly and fairly scheme proposed rate regulation algorithm, resulting analysis of proposed mechanism describes that it is good and high performer compare to the previous one same link is share signal fairly without getting any problem regardless of flow and error control services , result show that TRMCC model is specially impactable in the network that works on intra session environment with the cooperation of WSN friendliness and scalability measurement scenario has been looked after their cause proposed scheme is meaning full and effective for the WSN Error problem occur at dynamic network.

In [8] proposed an evolution model with the aim to get effectively utilize the sensor network nodes capacity, here author gets concentrate on how amplify the sensor power during the process to get reliability in communication for long distance range, so that they proposed an inherent algorithm which process buffer computation at every node to get process node to node interact effectively using their own nodes power so that we can have more strong WSN compare to previous one, in [10] author primarily focused on the issues occurred due to network pattern mismanagement which leads delay and interruption in between the process so author realizes it happen due to different network pattern so that they design an new approach to get manage such dynamic pattern to eliminate disputes. In[7] author proposed SAODV routing protocol for WSN which address the solution of secure routing in sensor network this protocol has been designed to resolve the problems found in traditional AODV protocol so that one can say it is the extension of AODV , SAODV process secure routing by protecting the route used for the delivery first then do the next thing the specialty of SAODV is its secure key management system where every node having their individual public key for the purpose of authentication and verification of the message for security reason. In[9] author measure the effect of Flood attack in WSN during routing process, NS2 simulation defines that with AODV WSN has less Flood impact as compare to the other black hole attack for the measurement of performance of overall network. In[4] one analyses the effect of Black hole, Gray hole, Flood attack along with the implementation of PDF and other protocol over WSN for the hop count and data loss measurement purpose, here one found that Flood causes delay whereas other attack effect on data loss and delivery ratio.

## III. CONCLUSION

literature based analysis of related papers and existing proposed schemes, since to find actual problems and errors in present technology it is always necessary to analyses the relevant paper from reliable sources like IEEE and ACM etc., to keep and find specific objective related to the thesis work has been done by the author by the help of this Section. After going through the large number of related literatures author gets the actual area of problem raised during communication of peer to peer network , how attacker get enter into the system and attack over the server during process therefore it is always required to get solve such issues before proceeding the network operations.

## REFERENCES

[1] S.Uma maheswari, N.S.Usha, E.A.Mary Anita, K.Ramaya Devi, Published paper titled as “A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN” in IEEE International 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 SensorNetworks - 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] Sunil Kumar Singh,” A Survey On Successors Of Leach Protocol” IEEE Access vol. 5, 2017, pp 4298-4328,DOI: 10.1109/ACCESS.2017.2666082
[6] Nikos Bizanis, Fernando A. Kuipers,” SDN And Virtualization Solutions For The Internet Of Things: A Survey” vol. 4, 2016, pp 5591-5606, DOI: 10.1109/ACCESS.2016.2607786.
[7] D. Cazorla, et al., Model checking wireless sensor network security protocols: Tinysec + leap. In Proceedings of the First IFIP International Conference on Wireless Sensor and Actor Networks (WSAN‟15), pages 95–106. IFIP Main Series, Springer, 2015.

 

[8] C. E. Perkins, "The Ad-hoc On-Demand Distance-Vector Protocol (AODV)" Ad-hoc Networking, Addison-Wesley, pp. 173–219, 2001.
[9] Farooq Anjum and Petros Mouchtaris,"Security for wireless Ad-hoc networks," John Wily, 2007.
[10] Humaira Ehsan, Farrukh Aslam Khan et. Al., "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 25-27 June 2012.



 