International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

OPTIMIZED ROUTING AND DENIAL OF SERVICE FOR ROBUST TRANSMISSION IN WIRELESS NETWORKS

Vivekanandan G[1], Saravanan A[2], Sham Christopher A[3], Yashwanth ram D[4] ,Yogamahi V[5]

[1]Assistant professor(O.G), Department of IT, SRM Valliammai Engineering College, Tamilnadu, India
[2,3,4,5]UG Students, Department of IT, SRM Valliammai Engineering College, Tamilnadu, India

---

Abstract - *Projects based on the cloud domains are increased in the recent years even though there are some security threats on the networks and data. One of the cyber attacks is Distributed Denial of Service attack, it is considered as the second most predominant attack in the information theft. These attacks can exhaust the power, bandwidth and all cloud resources. It causes end to end delay and connectivity problem in the network and affects the Quality of Service (QoS). Prevention and detection of DDoS attacks are vital roles in cloud domains. In this paper we are introducing a classifier system for detection of DDoS flood attacks which is named as CS_DDoS. It offers a solution to secure data by classifying packets as malicious packets and normal packets. It makes decisions based on the classification results. And the packets which are noted as an malicious will be blocked from the network and IP will be blacklisted. And to prevent a data and information we are performing efficient and quality routing technique with the use of Hybrid Optimization System (HOS). This will increase the lifetime of the network and leads the users to effective and energy efficient communication.*

***Key Words*: DDoS, CS_DDoS, , Detection phase, Flood attacks, QoS, Genuine flow and Malicious flow.**

1. INTRODUCTION

Background of the project: Middle-Box detection technique: Middle box is one of the detection techniques which is used to detect DDoS attacks in conventional system but it requires customized hardware and software, So it fails to maintain global intelligence in networks.

Differentiate between flow: Detecting the DDoS is hard without affecting the resources. It has the need to find out that incoming flow is malicious flow or genuine flow .

Routing: Detection of the attack is the part of the process, we have to use the routing technique to transfer the data from one node to another node. Basically data are transfer in static path, It makes easy for the attackers to make an DDoS attacks and to access their systems. And it makes the system slow when the attack is occurred or detected and it will lead to inefficient communication.

1.1 STATEMENT OF PROBLEM:

In the time of study for the project we noted that the DDoS attack detection technique has some of the drawbacks like not identifying difference between genuine flow and malicious flow. Multiple ports connected on the single switch, which is also called as dump switch is one of the reasons. And also having the low ternary content addressable memory (TCAM) slow down the searching of contents. DDoS attack affects the performance of the integrated network's throughput, delay and delivery ratio which is evaluated in terms of Data Packet Delivery Ratio (DPDR), Control Packet Overhead (CPO) which scales the total number of control packets from the total number of packets within the network. In Data Packet Delivery Ratio (DPDR), the ratio is calculated by the total number of effectively-transmitted packets to the total number of data packets transferred from the source to the destination. It also decreases the capacity of load balancing of the system. It results in the packet drop, which means that is the ratio of unsuccessfully transmitted packets sent from the sources.

1.2 AIM AND OBJECTIVES OF THE PROJECT:

The main aim of the project is to detect the DDoS attack in the very efficient manner and also prevent the data by the routing techniques, and it also important that the routing technique has to be efficient and it have to save our time than the other techniques, we have to find the shortest path to find the nearby nodes to transfer the data between them. The process has to repeat when the attacker attacks the redirected node. So that we are creating the multiple paths to make the process of finding path tougher.

The main objectives of the project are:

- To design an effective Detection and Routing technique for identifying the fake flows (malicious flow) and to transfer the data in other path without affecting time and content.
- The objective of the Routing and Detection technique is to removal of fake traffic and the delay in networks and to find the duplicate data.
- And to perform cost effective routing technique which takes less time to transfer the data from source to the destination without losing data.

2. RELATED WORK:

This section presents previous work related to our proposed architecture. We have highlighted some of them to identify the significant attributes of these systems.

Tolga Numanoglu et al [1] al in this paper he studies about the coordinated and also non coordinated MAC protocols and the performance with respect to the result of channel noise. Due to the control traffic dependence and BER level the performance loss and the vulnerability in the coordinated MAC protocol is higher when it's compared to non coordinated MAC protocols.

Bulent Tavli and Wendi B.Heinzelman et al [2] In this paper he describes about the super frames and also nee proposed MH-TRACE, super frame is a frame which consist of multiple time frames, to transmit the packets cluster have to choose the any frame . Anyway all the nodes are receive the targeted packets in the range according to the formed clusters. This paper results in the each nodes create clusters to receive the packets it wants and then it declared that the throughput of carrier sense MAC protocols are lower then the MHTRACE protocol.

Mikko kohvakka et al [3] This paper is morely based on the peer to peer topology which focuses on the energy consumption in the network. There are several models described in this study like Multiple access control and the CSMA-CA mechanism and also ZigBee. The need of the paper is to analyze the power and throughput of the network which are checked by the WISENES. It results that the minimum power utilized is 73 μW and the beacon interval is 3.93 s.

Sung-Hwa Hong et al [4] He proposed the mechanism called as an duty cycling which is used to achieve the energy efficiency in the wireless sensor networks, in the previous projects the exchange between the latency and the energy efficiency is the only remained issue. So In this paper he proposed the Express MAC which strongly imposes the need of end to end latency when saving the energy. It can also able to access the applications in the multi hop with the use of cross layer application program interface. It is an proven method that EX MAC is able to Ensure latency and wakeup time.

Jun Guo et al [5] He briefly studied about the TDMA model's waiting time and the density distribution with the state dependent service. The solidity of the interval with the combination of beta allows efficient recursive scheme. Queuing method is used to express the waiting time and he also proposed the methodology which treats the special issues in the previous papers.

Kazem Sohraby et al [6] In this paper we studied some of the unique features in the wireless sensor networks. This paper briefly presents review about the transport protocols and some of the challenges and basic designs in it. And also the writer discussed about some of the open research problems.

Jing Zhu et al [7] Author anticipated that what are some of the specifications needed to modify the multi-hop connectivity, so he provides the overview about the dedicated short-range communication (DSRC) and their requirements. And also provides the variety of QoS and highlights some of the issues.

Stavros Toumpis et al [8] This paper analysis about the CSMA that is carrier Sense multiple access and compares with the power control MAC and the CA protocol. And it's result that the routing protocols are performs better then the Carrier sense multiple access protocol and the power control MAC. In the terms of an energy efficiency POBA is better than the other two protocols.

Bora Karaoglu et al [9] This paper explains about the mobile ad hoc network and it success which fulfill the specific requirements of the networks and the better use of the channel resources. The dimensions of this technique is that when the space increases the power of processing also increases. He addressed the relationship between the overall performance and the parameters of the protocols. This paper presents the model for the effective parameters by increasing the number of frames and also wants to predicts the conditions.

3. PROPOSED WORK:

In our modified proposed system we are focusing on factors mainly efficient reliability and the maximum time of the network in the ad-hoc network (wireless). We are providing the energy knowledge routing algorithm called as consistent or reliable minimum energy cost routing that is RMECR and it is used to find the consistent route which is energy efficient that used to maximize the duration and lifetime of the network communication, we are using an deep and detailed analytical model for the energy expenditure of the nodes. It has the property of hop by hop (HBH) which used in link layer consistency and the E2E retransmission reliability. The hop by hop is acceptable by the MAC layer to increase reliability of the links. Some of the MAC protocols are not acceptable by the HBH retransmission in this kind of E2E retransmission could be used to ensure reliability of the network. Load distribution (non uniform) and the spatial reuse which is very strongly linked to the bandwidth efficiency are the main obstacle when using the MAC protocol. When we use the Spatial reuse will drastically increase the efficiency of bandwidth, on the other side the traffic load is mostly non uniform which is the critical part that the protocol be able to handle traffic efficiently, this happens due to the dynamic behavior in the mobile networks. These Un co-operative protocols are incorporated with the spatial reuse and to make itself ready to handle the

load distribution through the carrier mechanism. The careful design of the MAC layer will make way to the changes in the traffic distribution. As like the cellular system and the combined mobile network and the MAC protocol needs some of the channel mechanism that is borrowing mechanism that noticed the characteristics of the mobile network to provide the advantages like increasing the bandwidth and their Un-assembled counterparts. MANET are having some of the dynamic nature the network load is not uniformly distributed. We have to cope the non-uniformed distribution that is load distribution in the mobile networks so we are proposing the algorithms namely the less weight distribution allocation (Dynamic channel) and based on the availability of the resource nodes are need to select the channel access providers, so the alloy called coordinative load balancing algorithm are used.

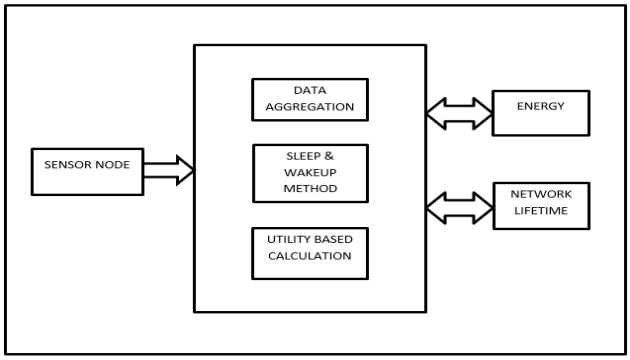

Fig. 1. System architecture diagram for proposed system

MH-Trace framework manages the load distribution, but it don't provide any of the support to change the conditions and the formations of the load. Tough we use this algorithm for creating the new protocols with the CDCA and CMH trace.When the MH-TRACE are enables the dynamic assignment and also the scalable assignment the CDMA-TRACE are used to maintain the same energy level and the efficiency. It also keeps the tracks of the nearby clusters to utilize the spectrum sensing feature makes sures the cellular networks make the CDCA Is more suitable for the MANET.

In the MAC protocols under the non uniform load, it is more critical to flexible enough to let the bandwidth which are unused into the controllers of the highly loaded regions. The mechanism of the dynamic channel allocation is similar to the cellular system which is already exists and perform the channel allocation between the cell towers. By adopting this utilizes the spectrum sensing and the message are cost too much for a mobile network.

The person who is controlling the channel has to monitor power and the availability asses in the channels by contrasting with the threshold levels. When the threshold level increases over capacity it motivates the coordinator. Then he has to increase the power level of that channel which safeguard them to access the same channel.

In this algorithm maximizing the bandwidth seeks the attention of the channel coordinators. It is effective in terms of providing the support and the response by the coordinator will increase entire interference.

From the perspective of channel coordinators the DCA Algorithm approaches the problem of non uniform load distribution. The same problem can also be approached from the perspective of ordinary nodes. Without the need of coordinator side the cooperative behaviour clears non-uniformities in the load distribution. To monitor the channel usage and the active nodes load balancing algorithm is used and it switch the heavy load from coordinator and depleted their channel load. This increases throughput and the total no of nodes that access the channel

Mesh routers has the minimal number of mobility and no constrains, so the routing protocols in there are expected with some of the changes like change in size when it's compared to the ad-hoc networks, routing for the clients are more easy with the use of infrastructure build in.

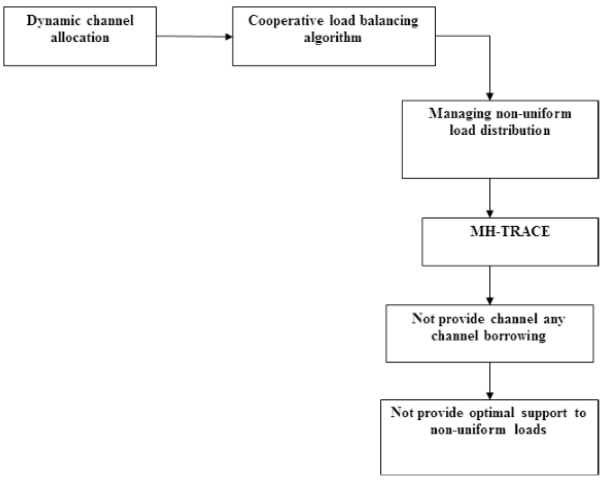

Fig. 2. Data Flow diagram for proposed system

The performance level of protocol has the legitimate impact in the LQSR that is link quality source routing. There are some of the performance levels in the LQSR they are the expected transmission count, per-hop packet pair and the per-hot RTT. This performance will be calculated and compared with the least and the minimum hop count codes to achieve the better performance. This will be result in the link quality metrics and it's not enough for the WMN where the mobility is considered.

4. METHODOLOGY:

DDoS is an attack is process of creating the fake network traffic with the use of malicious software which are spread in the cloud domains to affect the data, all the botnets perform the same kind of malicious function. They are performing this attack by the fake IP address to make themselves untraceable. There are some of the reasons to perform this attack like cloud based competition or any revenge and also for fun. DDoS attack points the weakness of the cloud and attack precisely. This attack in the cloud may be either internal or external.

In this paper we are using the new scheme called as the Hybrid Optimization System for performing effective and efficient connections through routing techniques. This HOS system consists of some of the advantages like dynamic routing and multi path scheduling and strong transmission to overcome the attacks in the network. It also minimize the faults in the node levels to increase end to end connectivity and to balance the load to maintain the stable and static transfer between source and destination. It also performs well in terms of packet delivery ratio, average delay time and also in throughput.

4.1 DDoS Attack Detection

When we do the data transfer in the software defined network there is a threat in three planes of that network. All the three planes of SDN architecture namely Controller plane, Application plane and Data plane has some of the threats for the attacks like space constraint in the data plane causes the buffer saturation, this is due to the presence of multiple ports interconnection. So in this work we are building the efficient and effective Intrusion Detection System (IDS) this proposed work leads the user for the high speed and the secure communication. In our system we are featuring the use of anomaly detection and the Network Function Virtualization technique, the lightweight anomaly detection based on the single feature is best for the software defined networks we are also using the open virtual switches in the detection system to virtualize the path, moreover it helps to track the abnormal traffic, which can be applied in many areas.

Each of the nodes send their route request to the neighbour nodes to know if it is the destination if not that second node sends the request to their neighbour node, this process will continue until the destination is identified, after finding the destination, it will send the route response to the source and the system will scan the path for if any of the malicious nodes are containing. The system calculates the threshold energy with the use of anomaly detection and TCAM memory, when threshold level increases above the limit it will report as an attack and our routing technique takes place. If no nodes are giving the response it will be addressed as route error or broken links.

4.2 Routing

This is the process after we detect the attack, we have to redirect the static path into the other if not it leads to the data loss so we have to perform routing. For that we are using routing algorithm for performing the routing in the efficient manner.

Ad hoc on demand distance vector routing technique is used in this process it is mostly used in the mobile ad hoc networks and also it is capable to perform both unicasting and also multicasting. This algorithm builds the routes between the source and destination nodes. It also forms the trees which are composed of some numbers and to ensure the nodes doesn't get affected. It also capable for looping and self formation for the large number of mobile nodes. Then Open shortest Path Algorithm is used to find the path which has the minimum distance to reach the destination. The design is based on wireless sensor networks which can change dynamically, it looks as deployed in initial condition but when the process finished it consist only of the disconnected parts .

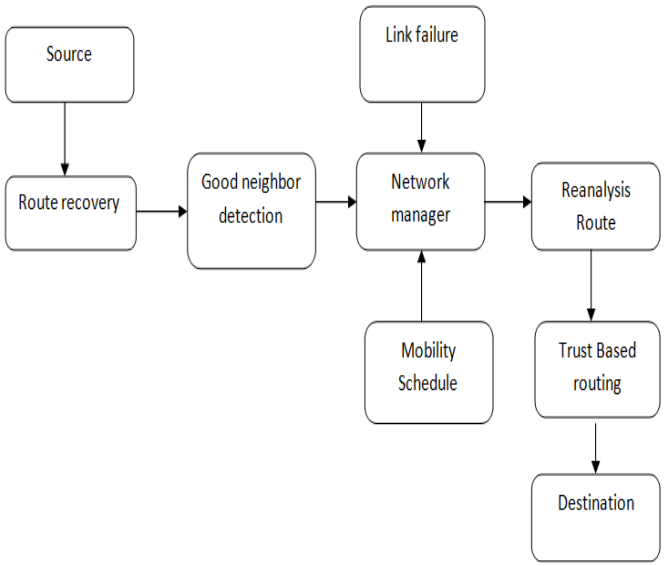

Fig.3.flow diagram for routing process

5. Hardware and software components

The following section is used to describe about the components used in this system

A. Hardware Requirements: We are using the intel processor Pentium IV series with 2.4 GHz and our system has the hard disk of 40 Gb in the Monitor which has 15 VGA Colour, Mouse and Ram of 512 Mb.

B. Software Requirements: Operating System: This project can be done in the Windows XP/7/10/LINUX, and this is implemented in NS2 in the Version of 2.28. In the Front End we are using OTCL (Object Oriented Tool

Command Language), Tool: Cygwin (To Simulate in Windows OS)

C. NS2: NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2.

D. Operating System: Ubuntu 10.04(LINUX): Ubuntu is a Linux distribution based on Debian and composed mostly of free and open-source software. Many additional software packages are accessible from Ubuntu software as well as any other APT-based package management tools. Ubuntu is officially released in three editions: Desktops, Server and Core for IOT devices and robots. All the editions can run on the computer alone or in a virtual machine.

E. WorkStation Tool: VM Ware Workstation Pro 12.1-VM Ware workstation supports bridging existing host network adapters and sharing physical disk drives and USB devices with a virtual machine. VM ware Workstation Pro can save the state of a virtual machine (a "snapshot") at any instant. It can simulate disk drives an ISO image file can be mounted as a virtual optical disc drives and virtual hard disk drives are implemented as dot vmdk files. These snapshots can later be restored effectively returning the virtual machine to the saved state as it was and free from any post damage to the VM.

F. Designing Language: TCL (Tool Command Language): TCL is a scripting language for controlling and extending software applications. You can run TCL console windows with the TCL Scripts command on the tool menu or tasks in the Task windows A .TCL file contains a TCL script which is composed of TCL function and can also include Quartus prime application programming interface (API) functions used as commands.

G. Protocol Design: C++ is a programming language which allows the programmer to instruct a computer to use system resources and memory. C++ is adaptable to multiple platforms.

6. EXPERIMENT AND RESULT:

In this experiment, results of our implemented system as well as the relevant details. This output can be divided into five consecutive parts which work together:
A) Creating multiple nodes
B) EAACK process
C) Data Transfer from source to destination
D) EAACK- Ack process
E) Dynamic Source Routing

A. Creating multiple nodes:

Between the source and the destination nodes we have to create intermediate nodes using the network virtualization function and the open switch. Multiple intermediate nodes are created for the routing if the attack takes place the intermediate nodes. All the intermediate nodes are virtualized within the static path. The destination also not initialized between the nodes, it will be identified by requesting neighbour nodes until it finds the destination.

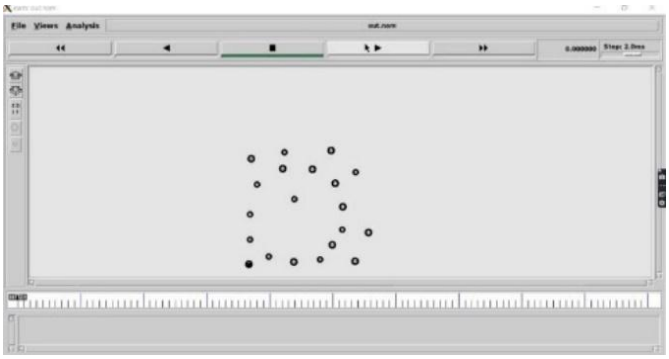

Fig. 4 Creating multiple nodes

B. EAACK Process:

Enhanced Adaptive Acknowledgment (EAACK) it is used to perform the defense mechanism for the packet attack. It is the intrusion detection system detecting the neighbour nodes to find the destination node and also checking the nodes that if contains any malicious nodes or not.

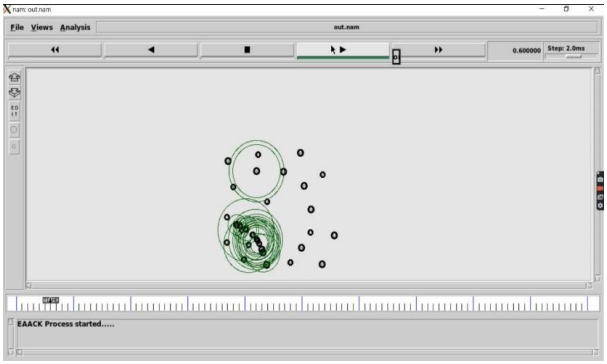

Fig. 5. EAACK Process

C. Data Transmission from source to Destination

Previous process is used identify the source node and destination node. In this process each nodes searches for the nearby nodes that if they contain malicious function if not it continues the static transmission if not it acknowledges the system.

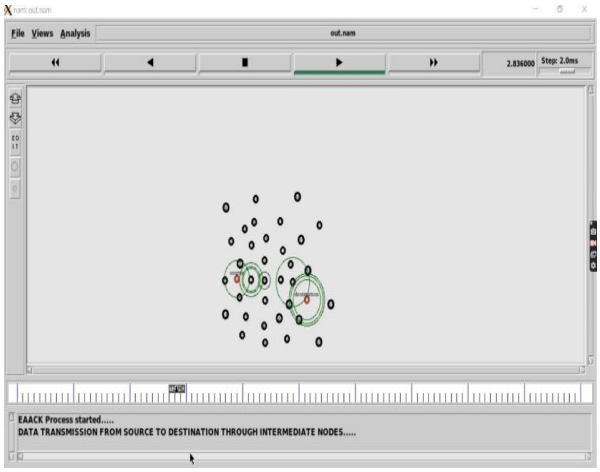

Fig. 6. Data Transfer from source node to destination node

D. EAACK-ACK

After analysing the neighbour nodes there is a need to acknowledge the system that there is no malicious node or if any malicious nodes are identified it also mandatory to acknowledge to process the routing technique. The intrusion detection system has the acknowledgment part which takes place after analysing the nodes.

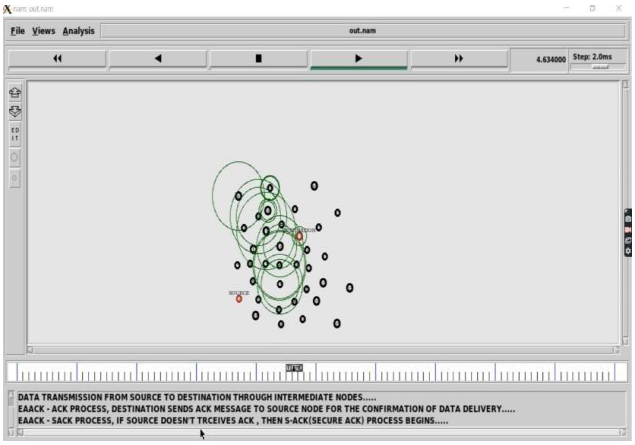

Fig. 7. EAACK-ACK

If the malicious nodes are identified the nodes are highlighted and the next process of routing will be takes place.

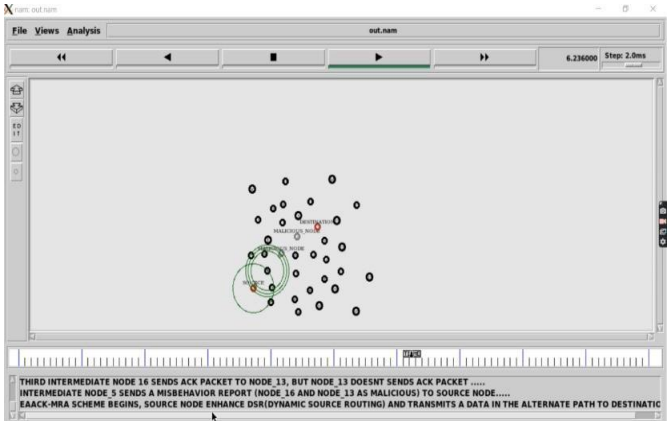

Fig. 7.1. EAACK-ACK if attack is identified

E. Dynamic Source Routing

When the acknowledgement came that the path contains the malicious nodes dynamic routing will be processed with the mentioned algorithm of Ad-hoc on demand Distance algorithm and with the use of the open shortest path algorithm.

This algorithm finds the shortest way to reach the destination node and then it analyze the newly founded path that to verify that there is no malicious nodes is the new path.

If any nodes are identified it will alternate the path till system finds the path without any malicious flow. After finding the secure path static data transmission is used, each of the nodes *only have the info about the previous* and the next nodes so it makes tough for the attackers to find the path.

7. CONCLUSION:

This project results in the effect on the routing layer we are not investigated the effects and we focused on the MAC layer about that capability and service like broadcasting in the local level. Packet has the significant impact based on the load distribution.

Network flooding is using the local link broadcasting along with the network coding. As conclusion joint optimization of the MAC and the routing layers can make the better solution. And the effect of the routing is left as the future work.

8. REFERENCES:

[1] Lifei Huang and Ten-Hwang Lai. On the scalability of ad hoc networks. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing,

ISBN:1581135017
DOI:10.1145/513800

[2] Xin Ming Zhang, Yue Zhang, Fan Yan, and Athanasios V.Vasilakos. "Interference-Based Topology Control Algorithm for Delay-Constrained Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING.

ISBN: 14965390
DOI: 10.1109/TMC.2014.2331966

[3] R. G. Li and A. Eryilmaz, "Scheduling for end-to-end deadline constrained traffic with reliability requirements in multihop networks".

ISBN: 13039045
DOI: 10.1109/TNET.2012.2186978

[4] M.F. Neuts, Jun Guo, M. Zukerman, and Hai Le Vu. The waiting time distribution for a TDMA model with a finite buffer and state-dependent service.

ISBN : 8584479
DOI: 10.1109/TCOMM.2005.855014

[5]Mikko Kohvakka, MauriKuorilehto, Marko H¨annik¨ainen, and Timo D. H¨am¨al¨ainen. Performance analysis of and zigbee for largescale wireless sensor network applications. In Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks.

ISBN:1595934871
DOI: 10.1145/1163610

[6] B. Tavli and W. B. Heinzelman. MH-TRACE: Multi hop time reservation using adaptive control for energy efficiency. IEEE Journal on Selected Areas of Communications

ISBN: 8111623
DOI: 10.1109/JSAC.2004.826932

[7] P. Li, C. Zhang, and Y. Fang, "Capacity and delay of hybrid wireless broadband access networks"

ISBN: 10469657
DOI: 10.1109/JSAC.2009.090203

[8] Chonggang Wang, K. Sohraby, Bo Li, M. Daneshmand, and Yueming Hu. A survey of transport protocols for wireless sensor networks

ISBN: 8944364
DOI: 10.1109/MNET.2006.1637930

[9] Bianchi. Performance analysis of the distributed coordination function. Selected Areas in Communications

ISBN: 6584745
DOI: 10.1109/49.840210

[10] SangkyuBaek and Bong Dae Choi. Performance analysis of power save mode infrastructure WLAN In Telecommunications

ISBN: 10364438
DOI: 10.1109/ICTEL.2008.4652710