November-December 2019
ISSN: 0193-4120 Page No. 4690 - 4694

# Event Aware and Attacks Detection by using Optimized Link State Routing (OLSR) Protocol

M. Smitha
*Student, Department of Computer Technology, Sri Krishna Arts and Science College Coimbatore, Tamilnadu, India. (Email: smitham18mct012@skasc.ac.in)*

S. Nandhini
*Assistant Professor, Department of Computer Technology, Sri Krishna Arts and Science College Coimbatore, Tamilnadu, India. (Email: nandhinis@skasc.ac.in)*

J. Aiswarya
*Student, Department of Computer Technology, Sri Krishna Arts and Science College Coimbatore, Tamilnadu, India. (Email: aiswaryaj18bct005@skasc.ac.in)*

M. I. Rofina Begum
*Student, Department of Computer Technology, Sri Krishna Arts and Science College Coimbatore, Tamilnadu, India. (Email: rofinabegumi18bct041@skasc.ac.in)*

***Article Info***
***Volume 81***
***Page Number: 4690 - 4694***
***Publication Issue:***
***November-December 2019***

***Article History***
***Article Received:*** *5 March 2019*
***Revised:*** *18 May 2019*
***Accepted:*** *24 September 2019*
***Publication:*** *23 December 2019*

***Abstract:***
In this paper we say about the entire activities of OLSR protocol and how the attacks are being occurred during the networks, how the malicious node to be rectified, how the nodes more efficient to transfer the packets, if they find any malicious or suspected node in the packets they will rectify the malicious nodes and it will send to the correct destination. Ad Hoc networks play the major role in these kind of networking activities. MPR selection is one among the part of transferring the node from source to correct destination. Event aware and attacks detection my using Optimized Link State Routing Protocol with effective range of atrocities of the networking deserved and this is mainly being used in the army and military services. It can be implemented in the order of two phases of networks.

***Keywords:*** *Ad-hoc networks, OLSR, MPR, Multipoint.*

## I. INTRODUCTION

Optimized Link-state routing protocols such as Optimized Link State Routing (OLSR) and this protocol will send the data nodes to the correct destination without any distractions made by the network it should handle any type malicious node and rectify the node in the correct manner and it will send the nodes. OLSR is the proactive protocol it is efficient than any other protocol in the networks it purely depends on network basis and it is only work when the network range is high and more efficient. This protocol finds the malicious node and it will have cleared all such nodes and it will transfer node this mainly used in satellite purposes, military areas so, these areas have widely takes part in this kind of process it will also detect event and attacks if they occurred during nodes transaction to make sure that the database does not remain unsynchronized for the long period of time periods of time. Like the name proactive it is very efficient and does not need any node to active this node. This is purely independent node of transaction process. This will need the

networks to be work faster than any other process. OLSR protocol has many advantages on being implanted on NS2 tool.

## II. EXISTING SYSTEM

In existing system, the algorithm is slightly slow and it will take more time to send packets through the networks. If they find any malicious nodes they will change the whole node path it will take more to transfers the node, it will check step by step first it will check the malicious node and it will rectify the node, and second it will change the path, by doing this the whole path will be changed and made that path more significant and more efficient after this process the path will be rectified nodes are transferred. By following oldalgorithm this process is followed time taken, identification of rectified nodes all will be changed and transaction process is done this will lead to more time and energy and networking should be more efficient and this will lead to many obstacles will lead this process in the network and transaction process is also gets some difficult. INSENS&SMECNS are the two main steps will provide better efficiency in transaction process in algorithm is used to transform the networks with appropriate nodes with particular time and efficiency.

*Limitations*

- Resources are very less.
- Physical security not that much high.
- Intrinsic mutual trust vulnerable to attacks.
- Authorization facility is less in OLSR protocol

To identify and detects nodes in OLSR protocol Volatile network is not preferable

## III. LITERATURE SURVEY

| TITILE | AUTHOR | YEAR | DESCRIPTION |
|---|---|---|---|
| **Security for node isolation attack on OLSR by modifying MPR selection process** | DeveshMalik ; Krishna Mahajan. | **2014** | In this work, they explain about the security nodes isolation takes place on attacks on OLSR protocol by modifying the MPR selection process this method is more efficient for processing the nodes in the desired manner. The modifying process will take efficient node will be transferred in appropriate time. |

| | | | |
|---|---|---|---|
| ➢ **Enhanced OLSR for defense against DOS attack in ad hoc networks** | MohanapriyaMarimuthu ; IlangoKrishnamurthi | **2013** | In this work, the enhancement of OLSR is done with this process we can able to overcome DOS attacks occurs due to Ad hoc networks. This DOS attacks is quite dangerous that is solve by using normal process that is only solved only by enhancing the OLSR protocol networks by using attacks detection. |
| ➢ **Performance assessment of OLSR protocol under routing attacks** | MahmoodSalehi ; Mehdi Dehghan | **2012** | The performance assessment of OLSR protocol under attacks this process will make the node more efficient to under taking the process of performance. Routing process of assessment is the ad hoc networks will make this process of any enhancement of networks of the process taken. |
| ➢ **DSR vs. OLSR: Simulation Based Comparison of Ad Hoc Reactive and Proactive Algorithms under the Effect of New Routing Attacks** | MahmoodSalehi ; HamedSamavati | **2012** | This paper talks about the comparison between DSR AND OLSR simulation networks this will also talks about the reactive and proactive algorithms under the effect of new routing protocols this will say about best points of pros and cons of new routing attacks of any algorithms pf any kind of networks. |
| ➢ **Mitigation of jamming attacks in wireless networks** | R. Dorus ; P. Vinoth | **2013** | This paper tells about the mitigation of jamming attacks in wireless networks it tells the overall process of the networks is being alerted in the many node of attacks of the it will find the malicious nodes of the networking attacks of the process denied. |

| | | | |
|---|---|---|---|
| ➢ **Delay of power control of routing and MAC protocol for Wireless Sensor Networks** | SandhyaRachamalla; AnithaSheela | **2015** | In this work we created a frame work for Power control and Delay aware routing and MAC control(PCDARM) for constraint of energy and sensitive sensor are delayed by using this we can able to reduce the Realability, Power efficiency |

## IV. PROPOSED PROTOCOL

OLSR protocol in nothing but Optimized Link State Routing Protocol it will send the data packets through the networks with various terminologies to be followed in that protocol through algorithm. This means the algorithm is very efficient in manner. The protocol which has been used in the network it should be enough sure and efficient manner to the configuration used. A node that does not have access to the shared secret key cannot produce a verifiable digest. In OLSR protocol the packet is send to source to destination if they found any path is getting disrupted by traffic in previous study they will change the whole node path so., this will take more time to send the packets through the networks. But in this proposed algorithm we found that if there is any malicious node the only particular node will be corrected and we will send that node in the correct manner further it will send to the correct destination without any traffic it will reduce time consumption and energy save.

## V. ADVANTAGES

➢ It does need any central administration system to handle it routing process because, it is a flat routing protocol.

➢ The proactive protocol provides all the routing information included in the network.

➢ It provides energy and time consumption.

➢ Flooding issues can be reduced by the MPRs, and its speed up the process of packet delivery.

## VI.PERFORMANCE ANALYSIS& RESULTS

OLSR is also a flat routing protocol, it does not need central administrative system to control its routing process. The effective characteristic of the protocol provides that the protocol has all the routing information to all participated hosts in the network. However, as a disadvantage of OLSR protocol needs that each host periodic sends the updated topology information and data throughout the entire network, this increase and brings efficient to the protocols bandwidth usage. But the flooding is minimized by the MPRs, which are only allowed to forward the topological messages.

## VII.CONCLUSION

In this paper, I have concluded that the event aware and attacks detection by using Optimized Link State Routing Protocol had been rectifying by using RSA algorithm with different methodologies each node is monitored and found the affected(malicious) node and cleared with the help of OLSR protocol. By doing this the time and energy are saved, the reduction of cost also has been reduced. The implementing part also designed in two phases of NS2 tool. Though it is wireless based Ad Hoc networks the we can use NS2 tool networks.

## REFERENCE

1. J. E. Paquet, “Guidance for Intelligent Transport Systems (ITS) in Urban Areas,” no. March, 2010.
2. Salaman G. “Performance Evaluation of OLSR Protocol AODV and VANET Cloud computing in 2005 Conference.

3. MahamoodSaheli: Mehdi Dehghan "Performance assessment of OLSR protocol under routing attacks, vol. 9, no. 4, December 2008, pp.389–408, doi: doi.org/10.1142/S0219265908002345.B. Kannhavong, H. Nakayama, N. Kato, A. jamalipour and
4. Mohanapriya; syderali,"OLSR Enhancement of automatic attacks on process denied." International Journal of Communication Systems, vol. 20, no. 11, November 2007, pp. 1245-1261, doi: 10.1002/dac.870.
5. Sandhyarachamalla,"Power-control delay aware routing and MAC protocol for wireless and sensor networks published in 2015 pp.1079-1084.
6. Mahamoodsalehi,HamedSamavati "Mitigation of jamming attacks in wireless network" published in the year 2012 of vol: 2.
7. DeveshMalik ; Krishna Mahajan. "Security for node isolation attack on OLSR by modifying MPR selection process. Published in the year of 2014.
8. IEEE Standard for Information technology-- Local and metropolitan area networks—Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6
9. C. Campolo, R. Scopigno, "From today's VANETs to tomorrow's planning and the bets," Vehicular Communications, vol. 2, n. 3, pp. 158-171, 2015.
10. J. Harri, F. Filali, "Mobility models for vehicular ad hoc networks: a survey and taxonomy," in IEEE Communications Surveys & Tutorials.