International Journal of Modern Developments in Engineering and Science
Volume 1, Issue 6, June 2022
https://www.ijmdes.com | ISSN (Online): 2583-3138


# Optimized and Secure Routing in WSN Using AODV and Optimized Routing Algorithm for DDOS Attacks

K. K. Sreedeve[1], R. Reni Hena Helen[2], I. Sree Varshini[3*], R. Deepika[4], B. Kalpana Sri[5]
[1,2]*Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*
[3,4,5]*Student, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*

***Abstract*: Due to the expeditious usage of the internet, network traffic and security challenges are increasing within the high-speed network. Though the IDS plays an important role in detecting potential attacks, the high volume of traffic creates significant technical challenges. DDOS attack can cause the node energy drained. As a result, node failures due to power limits generate system failures, which reduce network end-to-end connection. Furthermore, node mobility and congestion cause frequent link failures and packet losses, impairing the protocol's QOS performance. The Proposed scheme is hybrid optimization system and denial of service, for efficient routing and transmission for wireless networks. We are introducing a new classifier system technique to detect and block DDOS protocol flood attacks (CS DDOS). The suggested CS DDOS system provides a method for securing stored records by classifying arriving packets and making a decision based on the classification findings. CS DDOS recognizes and determines whether a packet is normal or originates from an attacker during the detection phase. Packets deemed as malicious will be denied access to the cloud service during the preventive phase, and the source IP will be blacklisted.**

***Keywords*: CS_DDOS, Distributed Denial of Service (DDOS), Intrusion Detection System (IDS), Quality of Service (QOS).**

## 1. Introduction

It's difficult to detect a DDOS without moving resources. It is necessary to determine whether the incoming flow is malicious or genuine. We have a tendency to ought to employ the routing approach to move the information from one node to any other node as part of the procedure of detecting the attack. Attackers can easily launch a DDOS attack and get access to their systems since information is shifted in a static way. And it slows down the system while the attack is occurring or being discovered, resulting in ineffective communication.

There has been an exponential increase within the power, frequency, severity, and volume of DDOS attacks despite the existence of all detection and mitigation solutions. Thus, the inevitable would like of the analysis community is to focus on developing an economical intrusion detection system (ids) framework against DDOS attacks with high detection power. The DDOS attacks are classified below the provision threat of the controller. The explanations for DDOS vulnerabilities are as follows: a) buffer saturation because of the restricted memory area to buffer the information, b) controller saturation is that the overhead in the controller due to the centralized design of the controller, c) flow table overflow because of restricted TCAM memory, and d) communication overhead of control-data plane link causes bottleneck to the legitimate users.

For wireless ad hoc networks, we present two innovative energy-aware routing algorithmic rules: RMECR (reliable minimum energy cost routing) and RMEER (reliable minimum energy routing) (RMECR). RMECR meets three critical requirements for ad hoc networks: energy efficiency, dependability, and network time extension.

It examines node energy usage and hence remaining battery energy, as well as link quality, to find energy-efficient and reliable paths that extend the network's operational lifetime. On the other hand, RMECR is an energy-efficient routing algorithm that discovers routes that use the least amount of energy for end-to-end packet traversal. RMECR and RMECR are designed for networks that rely on hop-by-hop or end-to-end retransmissions for reliability. Simulation experiments suggest that RMECR is capable of seeking out energy-efficient and dependable routes in the same way that RMECR does, while also prolonging the network's operational lifetime. As a result, RMECR is an ideal solution for extending the energy efficiency, reliability, and lifetime of wireless ad hoc networks.

Wireless communication has been around for over a century and has among the last decade become an everyday mode of communication in people’s everyday lives, because of the success of cellular and wireless local area network communication. Recently, researchers have centered on eliminating the requirement for fastened infrastructures in wireless communication, that has led to the event of ad hoc networks. A mobile ad hoc network (manet) additional considers node mobility within the ad hoc setting. Efficient use of resources and adaptation are important so as to make a high-performance manet. This treatise addresses the efficient use of network resources to get the desired quality of service and performance in MANET.

*Corresponding author: imdashack3r2001@gmail.com

## 2. Literature Review

Mäntylä and Lassenius., 2006; Schumacher et al., 2010; Santos et al., 2013. They measured the average end-to-end delay of CBR packets received at the destinations with increasing traffic load. Delay alone is concentrated. Advantage of this context, several machine learning algorithms have been adapted in order to enable an automatic detecting customization. The main disadvantage is Less detection method of DDOS attack.

Khomh et al., 2009; This algorithm describes the challenging problem of designing a scheduling policy for end-to-end deadline-constrained traffic with reliability requirements in a multi-hop network. The scheduling process is detailed in detail. The advantage of this context is procedure was created a single oracle containing 15 consensual smell instances. The main disadvantage is MIMO technology is used in hybrid wireless networks.

Khomh et al., 2011; Maiga et al., 2012; Amorim et al., 2015; Fontana et al., 2015. Description of this context, transmission power is minimized while keeping the connectivity and packet collisions are taken into account. Advantages are, the studies did not evaluate the efficiency of these techniques when customized from different training sets validated individually by single developer. The main disadvantage is they do not discuss about how such techniques deal on customizing the detection for different developers.

Maiga et al., 2012. In this they proposed three different algorithms with different complexity and characteristics. Advantage is Although defined by several developers, such oracles are not indexed by their evaluators. The main disadvantage is at end, the paper reported the algorithm was able to reach accuracies up to 0.78.

## 3. System Architecture

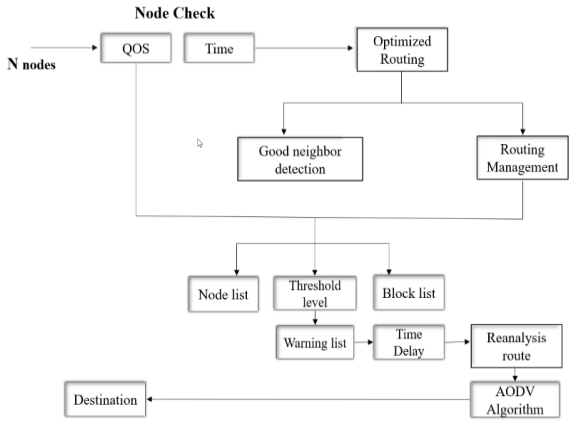


Fig. 1. Architecture diagram

## 4. Methodology

### *A. Creating Multiple Nodes*

Between the source and the destination nodes we need to create intermediate nodes. Multiple intermediate nodes are created for the routing if the attack takes place the intermediate nodes. The destination additionally now no longer initialized among the nodes; it will be identified by requesting neighbor nodes until it finds the destination.

### *B. DDOS Attack Simulation*

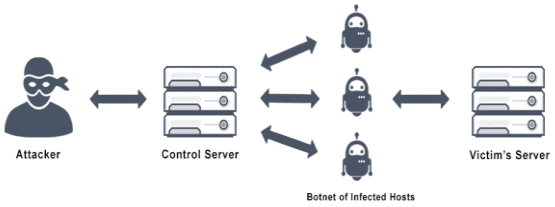


Fig. 2. DDOS attack

- *Attacker:* Attacker Send Request to the Control Server in order to Control an army of Botnets that floods traffic in the target network and shut down access to internet services and applications.
- *Control Server:* Control Server send request to group of botnets in order to execute the Malicious Program.
- *Botnets:* A centrally controlled group of infected or volunteered Computers(botnets) sends an onslaught of traffic to the target network.
- *Victim Server:* Here the Server can't handle the volumes of traffic and drop almost all packets from both good and bad Sources.

### *C. Detection of DDOS Attack*

Detection means abnormal traffic for data transformation. If data is transferring from source node to destination node once node attacked and abnormal traffic issues were there it will be detected by detection technique.

### *D. Alternate the Routing Path*

It is dynamic routing. In diversion we are used Ad hoc On Demand Distance Vector (AODV) routing algorithm. The shortest path routing algorithm is another name for it. This AODV routing algorithm is used to find the shortest path in in between nodes for packet transformation. This approach reduces the amount of time spent in the packet transformation pathway.

### *E. Path Check*

Filtration is nothing but it filters the pathway for packet transformation. This technique is used to find the traffic issues is there in path. This approach reduces the amount of time spent in the packet transformation pathway. Filtration always give valid path to the data transformation node. For example, if ten path is there for diversion then three paths had traffic issues and seven path not have issues then seven path only valid path for diversion.

### *F. Overall Performance Analysis*

In this Module, we will analysis the Performance of the Packet transformation between Source and the Destination process. The performance of the packet transformation is represented in the graphical format.

## 5. Results

This experiment presents the outcomes of our implemented system, as well as essential details. This output can be divided into five parts that work in tandem:

1) Creating a number of nodes
2) The EAACK procedure
3) Transfer of data from source to destination
4) EAACK- Ack procedure
5) Performance Analysis Graph

*1) Output for creating a number of nodes*

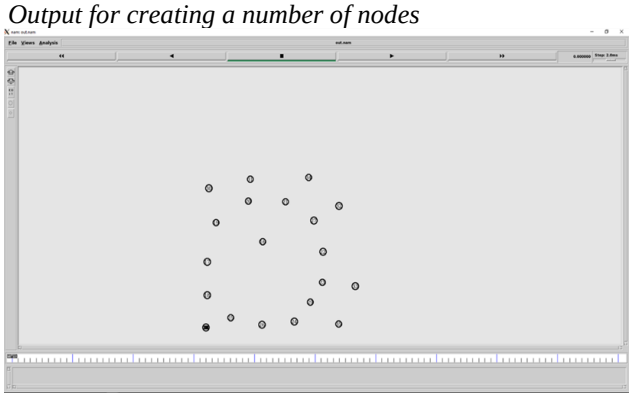

Fig. 3. Output for creating a number of nodes

*2) Output for the EAACK procedure*

Fig. 4. Output for the EAACK procedure

*3) Output for transfer data from source to destination*

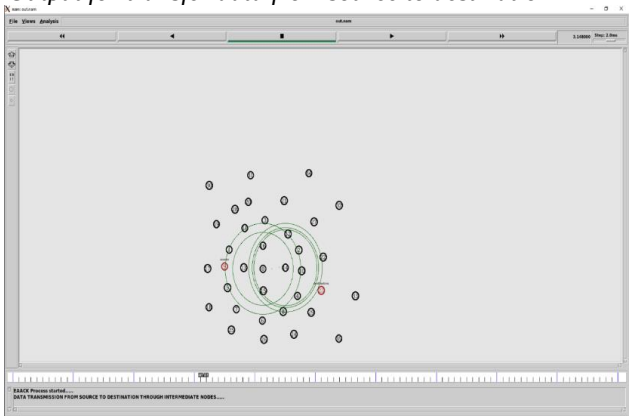

Fig. 5. Output for transfer data from source to destination

*4) Output for the EAACK-ACK procedure*

*Scenario 1:*

The Destination node will send ACK (Acknowledge) to the source node if there is no malicious node detected.

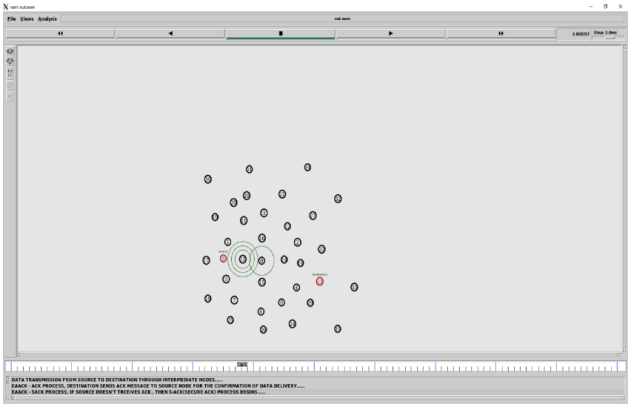

Fig. 6. Destination node send ACK to the source node

*Scenario 2:*

Step – 1: Detection of Malicious Node

If Malicious Node is Detected, then the node is marked as Malicious Node and change the path using Hybrid Optimization Scheme.

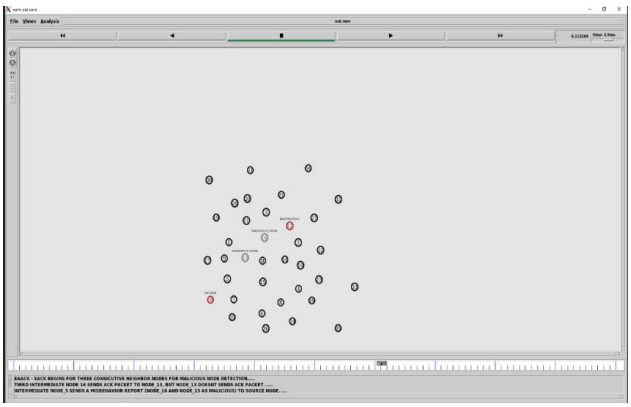

Fig. 7. Output for the detection of malicious node

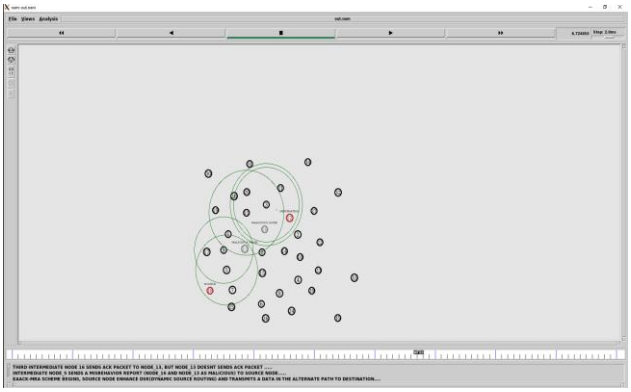

Fig. 8. Output for dynamic source routing

Step – 2: Dynamic Source Routing

When it is determined that the path contains malicious nodes, dynamic routing will be performed using the aforementioned Ad-hoc on-demand Distance algorithm and the open shortest path algorithm. This algorithm finds the shortest path to the

destination node and then analyses the newly discovered path to ensure that there are no malicious nodes on the new path. If any nodes are found, the path will be alternated until the system finds a path free of malicious flow. After determining the secure path, static data transmission is used; each node only knows about the previous and next node, making it difficult for attackers to determine the path.

*5) Performance analysis graph*

Scenario 1:

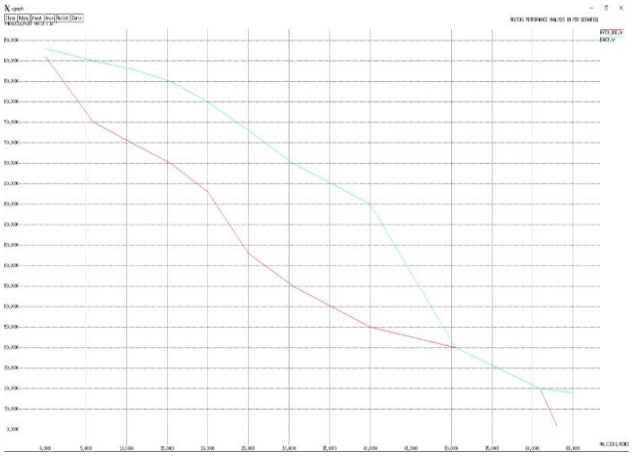

Fig. 9. Performance analysis graph for scenario-1

Scenario 2:

Fig. 10. Performance analysis graph for Scenario-2

## 6. Future Scope

In general, joint improvement of the mac and routing layers might alter even additional economical solutions. Investigation of the consequences of routing is left as future work. Collaborative routing is performed in WSN through optimisation and opportunities, that is enforced in 2 phases, collaborative node choice and optimization. within the 1st phase, the Lenient Constant (LC) is outlined and calculated which separates the probable collaborative nodes from the initialized nodes, supported parameters direct_trust, link strength and quality. These known collaborative nodes are solely allowed to induce concerned in the method of routing whereas the opposite non-suited nodes are merely restricted to require half in routing. within the second phase, optimization is incurred based on the proposed collaborative Optimized Routing algorithmic rule (CORA). Kore operates on the outlined Suit function (SF) that is modelled supported the parameters direct_trust, link strength, quality and therefore the distance.

## 7. Conclusion

In this project we've got not investigated the results of higher layers comparable to the routing layer, and instead targeted on the mac layer capability and local broadcasting service. Packet routing contains a vital impact on the load distribution. local link layer broadcasting service is directly employed by some routing algorithms such as network flooding. Moreover, it may be used aboard with network coding and simultaneous transmission techniques for cooperative diversity.

## References


[1] T. Numanoglu, B. Tavli, and W. Heinzelman. An analysis of coordinated and non-coordinated medium access control protocols under channel noise. Military Communications Conference, 2005. MILCOM 2005. IEEE, pp. 2642–2648 Vol. 4, Oct. 2005.

[2] A. Chandra, V. Gummalla, and J. O. Limb. Wireless medium access control protocols. IEEE Communications Surveys and Tutorials, 3:2–15, 2000.

[3] P. Mohapatra, J. Li, and C. Gui. Qos in mobile ad hoc networks. IEEE Wireless Communications Magazine, 10:44–52, 2003.

[4] 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, 22(5):942–953, June 2004.

[5] T. Cooklev. Wireless Communication Standards. IEEE Press, 2004.

[6] J. Karaoguz. High-rate wireless personal area networks. Communications Magazine, IEEE, 39(12):96–102, Dec 2001.

[7] T. Numanoglu, B. Tavli, and W. B. Heinzelman. The effects of channel errors on coordinated and non-coordinated medium access control protocols. In Proceedings of IEEE International Conference on Wireless and Mobile Computing, volume 1, pp. 58–65, Aug. 2005. 261.

[8] Bora Karaoglu, Tolga Numanoglu, and Wendi Heinzelman. Analytical performance of soft clustering protocols. Ad Hoc Networks, 9(4):635 – 651, 2011.

[9] Lifei Huang and Ten-Hwang Lai. On the scalability of IEEE 802.11 ad hoc networks. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, MobiHoc '02, pages 173–182, New York, NY, USA, 2002. ACM.

[10] IEEE 802.15.3 Working Group. Part 15.3: Wireless medium access control (MAC) and physical layer (PHY) specifications for high-rate wireless personal area networks (WPAN). IEEE Draft Standard, Draft P802.15.3/D16, Feb. 2003.

[11] Mikko Kohvakka, Mauri Kuorilehto, Marko H¨annik¨ainen, and Timo D. H¨am¨al¨ainen. Performance analysis of ieee 802.15.4 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, PE-WASUN '06, pp. 48–57, New York, NY, USA, 2006. ACM.

[12] M. Rahnema. Overview of the gsm system and protocol architecture. Communications Magazine, IEEE, 31(4):92–100, Apr. 1993.

[13] T. S. Rappaport. Wireless Communications: Principles and Practice. Prentice Hall, Upper Saddle River, NJ, USA, 2002.

[14] Jason Redi, Bill Watson, Ram Ramanathan, Prithwish Basu, Fabrice Tchakountio, Michael Girone, and Martha Steenstrup. Design and implementation of a mimo mac protocol for ad hoc networking. volume 6248, page 624802. SPIE, 2006. 262.

[15] V. Tippanagoudar, I. Mahgoub, and A. Badi. Implementation of the sensormac protocol for the jist/swans' simulator. In Computer Systems and Applications, 2007. AICCSA '07. IEEE/ACS International Conference on, pages 225 –232, May 2007.

[16] Heping Wang, Xiaobo Zhang, FaridNa¨ıt-Abdesselam, and Ashfaq Khokhar. Dps-mac: An asynchronous mac protocol for wireless sensor

networks. In Proceedings of the 14th international conference on High performance computing, HiPC'07, pages 393–404, Berlin, Heidelberg, 2007. Springer-Verlag.

[17] Jun Zhang, F.A. Nait, and B. Bensaou. Performance analysis of an energy efficient mac protocol for sensor networks. In Parallel Architectures, Algorithms, and Networks, 2008. I-SPAN 2008. International Symposium on, pp. 254 –259, May 2008.

[18] Sung hwa Hong and Hoonki Kim. A multi-hop reservation method for end-to-end latency performance improvement in asynchronous mac-based wireless sensor networks. Consumer Electronics, IEEE Transactions on, 55(3):1214 –1220, August 2009.

[19] Anna F¨orster, Alexander F¨orster, and Amy L. Murphy. Optimal cluster sizes for wireless sensor networks: An experimental analysis. In ADHOCNETS 2009: First International Conference on Ad Hoc Networks, September 2009.

[20] Chonggang Wang, K. Sohraby, Bo Li, M. Daneshmand, and Yueming Hu. A survey of transport protocols for wireless sensor networks. IEEE Network, 20(3):34–40, May-June 2006.

[21] Dawei Xia and NatalijaVlajic. Near-optimal node clustering in wireless sensor networks for environment monitoring. Advanced Information Networking and Applications, International Conference on, 0:632–641, 2007. 263.

[22] Ying-Ju Chen and Jin-Fu Chang. Per connection delay analysis of a frame based TDMA/CDMA mac protocol. Perform. Eval., 57(1):19–55, 2004.

[23] 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. Communications, IEEE Transactions on, 53(9):1522 – 1533, Sept. 2005.

[24] G. Bianchi. Performance analysis of the IEEE 802.11 distributed coordination function. Selected Areas in Communications, IEEE Journal on, 18(3):535 –547, Mar. 2000.

[25] Sangkyu Baek and Bong Dae Choi. Performance analysis of power save mode in IEEE 802.11 infrastructure WLAN. In Telecommunications, 2008. ICT 2008. International Conference on, pp. 1–4, 16-19.