European Journal of Molecular &Clinical Medicine,7(4):

Research Article

A Secured and Associated Congestion Hybrid AODA Protocol in WSN Networks using MANETS

ANANT RAM[1], JUGINDER PAL SINGH[2],

ANANT RAM[1], JUGINDER PAL SINGH[2],
[1,2] Department of Computer Engineering and Application, GLA UNIVERSITY, MATHURA, [1]anant.ram@gla.ac.in, [2]juginder.singh@gla.ac.in

Correspondence:

ANANT RAM[1]
Department of Computer Engineering and Application
GLA UNIVERSITY, MATHURA
anant.ram@gla.ac.in

ABSTRACT

Ad-Hoc Network is an independent arrangement of portable Hubs or nodes associated by remote associations. Hubs or nodes are free to travel, every now and again change their position and sort out themselves into a system. Hubs or nodes contain remote transmitter and beneficiary that permit them to participate in remote system. Hubs or nodes in MANET having double conduct, they go about as switches just as registering gadgets. Constrained transmission capacity and changing geography results the issue of Congestion in MANETs. Recognizing Congestion is troublesome in remote system, since there might be a few purposes for dropping of parcels. Specially appointed system is characterized as the system wherein the clients speak with one another by shaping a transitory system with no concentrated organization. Here every hub demonstration both as a host just as a switch. They have profoundly deployable, dynamic and self-configurable geographies. Different steering conventions are characterized for MANETs. Congestion and security issues are both solved in this paper using bloom filter and congestion aware protocol hybrid combination in AODV protocol. The results show better energy, PDR, throughput and high speed of the wireless sensor network.

Keywords: Secure, Congestion, AODV, WSN, PDR, Throughput, Delay, Replay attack.

DOI: https://doi.org/10.31838/ejmcm.07.02.03

INTRODUCTION

Systems have been rapidly making all through the latest couple of decades, varying from direct host-server structures to a thousand-center point WSN building. In equivalent, organizing threats have grown moreover. [1] The further developed the system, the broader the extent of potential network-based attacks or dangers that could be performed to upset the dedicated functionalities of that organize. [2] Replay network-based attacks or dangers are among the most widely recognized and easily performed network-based attacks or dangers. This line of investigation looks at the capability of Bloom diverts in tending to replay network-based attacks or dangers performed on remote sensor systems and how they field of WSNs is a productive wellspring of utilizations in industry, military, prosperity practices, coherent investigation, and various fragments. [7] Made out of practical sensors enacted by the general condition, influence essentialness, throughput, and amounts of packages exchanged the system. [3] WSNs, AODV directing show, replay network-based attacks or dangers, and Bloom channels are out and out ideas that make up the structure squares of my work, so we are discussed in detail in the going with subsections to give per users an unrivaled perception of the general contemplations and approaches.[4] WSNs are the eventual outcome of headways in the advancement fields of littler scope electro-mechanical structures (MEMS) and other related regions of investigation, for instance, correspondence arranges and introduced systems. [5] An insignificant exertion, less power requesting, space viable system structure is open for different uses and purposes. [6] The

WSNs can accumulate significant data, which would then have the option to be poor down for course of action purposes. [8] Data assembled by sensor systems are on a very basic level what the sensor center points perceive.

Sensor center points, as spoke to, it can separate light, heat, tenacity, sound, weight, or some other quantifiable sort of data that can be implied limit regards as demonstrated by what sort of sensor organize application is being utilized. [9] Mobilizers and power generators are not commonly utilized in sensor centers. As such, it is fundamental to have WSNs worked in an issue that ponders the ease of late referenced parts in order to keep up a commendable level of execution. [10] WSN center points can be passed on in self-assertive or fixed situations to fill the need of sending. Not at all like specially appointed systems, WSNs are for the most part the more thickly used, but then, they are inclined to disillusionments in higher frequencies than impromptu dispersions. Notwithstanding that, WSNs rely upon communicate correspondence. [11] Centers step by step gather their coordinating tables and start transmitting data subject to the courses they find; however impromptu systems are logically established on feature point correspondence. As for the size of WSNs, such a system comprises of center point numbers stretching out from tens to thousands in order to watch unequivocal consistent on the spot adjustments that may be shoreward, underneath the ground, or in wet situations, for instance, lowered or in soggy common environmental factors [12-14].

The overhauls in remote correspondence innovation empowered gigantic scope remote sensor systems (WSNs) arrangement. As a result of the capacity of simplicity of arrangement of sensor Hubs or nodes, remote sensor systems (WSNs) have a top-notch scope of projects which joins observing of general condition and salvage missions. Typically, remote sensor organize comprises of huge broad not many kinds of sensor Hubs or nodes. The all occasion is detected through the low vitality sensor hub which sent in arrange and the detected data is seeded to a base station [15-18]. To convey essential information from the environmental factors in genuine time it is unimaginable with wired sensor systems while remote sensor systems are utilized for records arrangement and preparing in real time from condition. The encompassing circumstances inside the environmental factors are estimated through sensors and afterward estimations are handled with a reason to decide the circumstance precisely in area over the sensors. Over a huge topographical territory enormous quantities of sensor Hubs or nodes are conveyed for precise observing. Due to the compelled radio scope of the sensor Hubs or nodes the upgrade in arrange size will build inclusion of territory anyway data (information) transmission for example Correspondence to the base station (BS) is made suitable with the help of middle Hubs or nodes [19,20].

IMPLEMENTATION

Now-a-days everywhere wireless sensor networks are using to monitor data from various fields such as health monitoring, military surveillance, monitoring temperature in agriculture fields etc. WSN networks are self-organizing which means they discover neighbor by themselves whenever they have to send data to destination, All WSN networks will use routing protocols to transfer data or communicate with one and other.

Routing protocol AODV helps WSN to find neighbors to reach destination, first source node will send RREQ (Route Request Packet) in the network and whoever nodes reach destination will reply to source as RREP (Route Reply) packet then source will use that route to send data to destination.

Existing AODV protocol does not include security features which make malicious node to perform replay (copycat which sends duplicate packet in the network which causes nodes to lose energy by reading same duplicate packets). All sensors work on battery and if battery goes down then sensor will die and network services will be disturbing.

To overcome from such issue in this paper author has introduce Secure AODV protocol which uses bloom filter technique to identify replay attack and once replay attack identified the node will simply drop such packets and can save energy.

Bloom filter uses array concept which fills with zeroes, suppose I used array of size 20 with index no

2 3 45 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0

Now I took packet data as ‘hello’ and then hash code of each character from the packet will find out and perform mod operation with given key. After mod operation whatever the values come then from above array 1 will be mark on the index of that mod value.

Example packet: ‘hello’

Hash code of character ‘h’ is 65

Selected key is 50

65 % 50 = 15 and from above array15th position will replace with 1and same will happen for all characters and bloom filter array will be prepared and if node send duplicate packet then same bloom filter will be generated and replay attack will be detected.

Here as simulation I design with two applications

WSN - This is a simulation application where nodes will perform route discovery and send data to sink node.

Sink Server - This application will receive data from WSN nodes.

In this project I have added metric to calculate PDR, Throughput and delay. As extension work, I added congestion aware technique to existing Secure AODV protocol. In congestion aware technique before sending packet, source node will send route request and all neighbors nodes will reply to route request with available congestion load on it. Source node will find those neighbor path which has less congestion on it. Source

node will send data to destination by choosing path which has less congestion.

In existing technique source will find shortest path to destination and send packet to it without concentrating available load on its neighbor path. If neighbor path already has lots of packets in it queue then there be huge response time which result into longer delay, less PDR and throughput.

To overcome from above problem, can choose path with less distance and less congestion so delay can be reduced. Fig. 1 to Fig. 5 shows the associated diagram as per paper algorithm implementation.

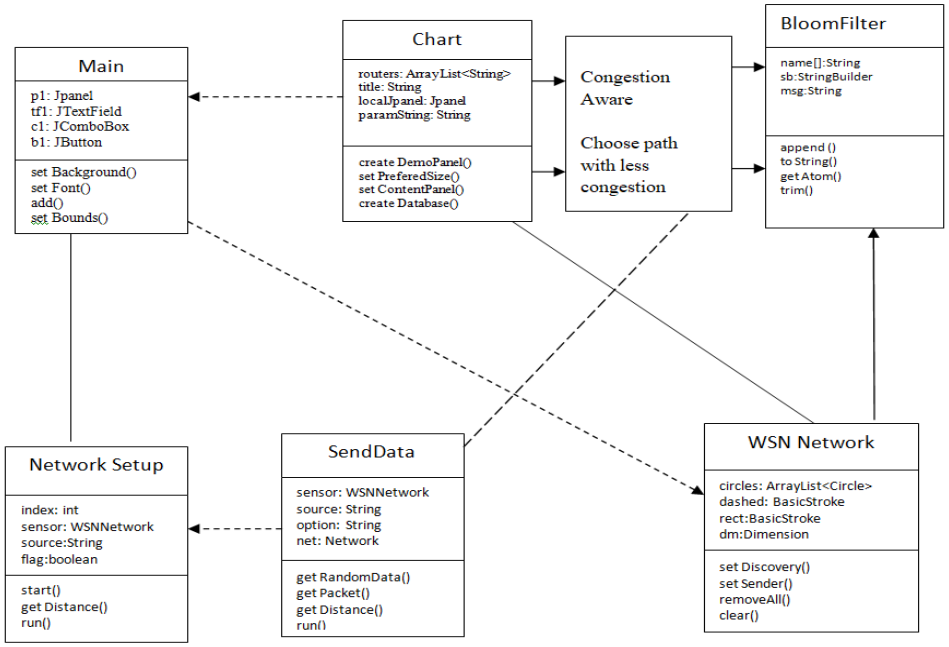

Fig. 1: Class Diagram

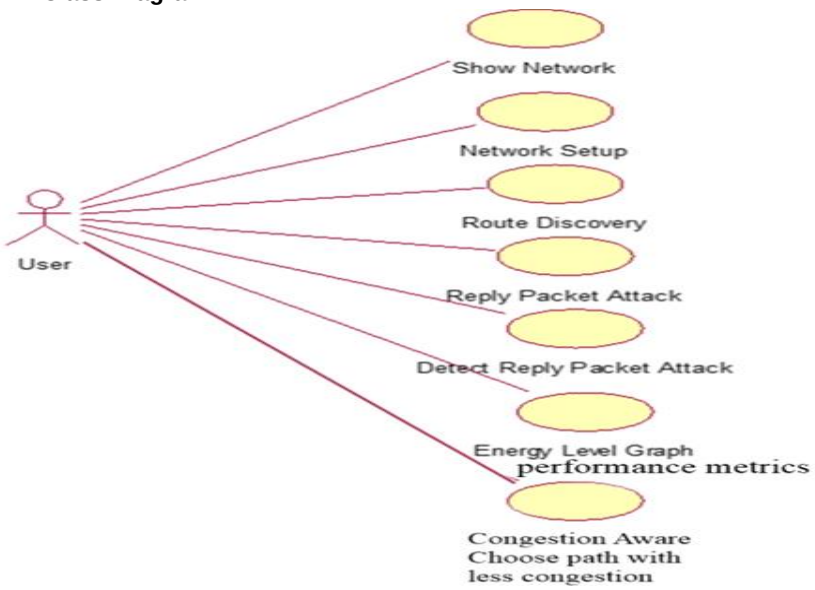

Fig. 2: User case diagram

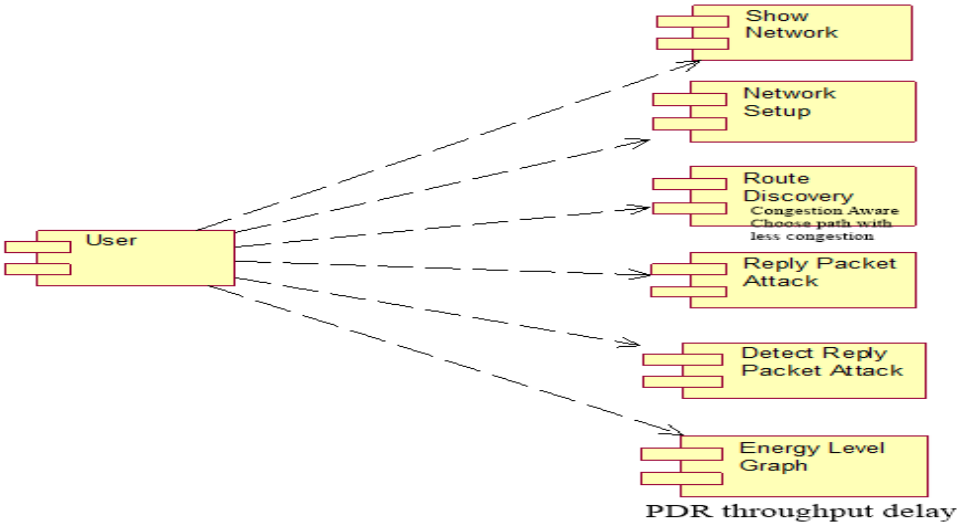

Fig.3: Component Diagram

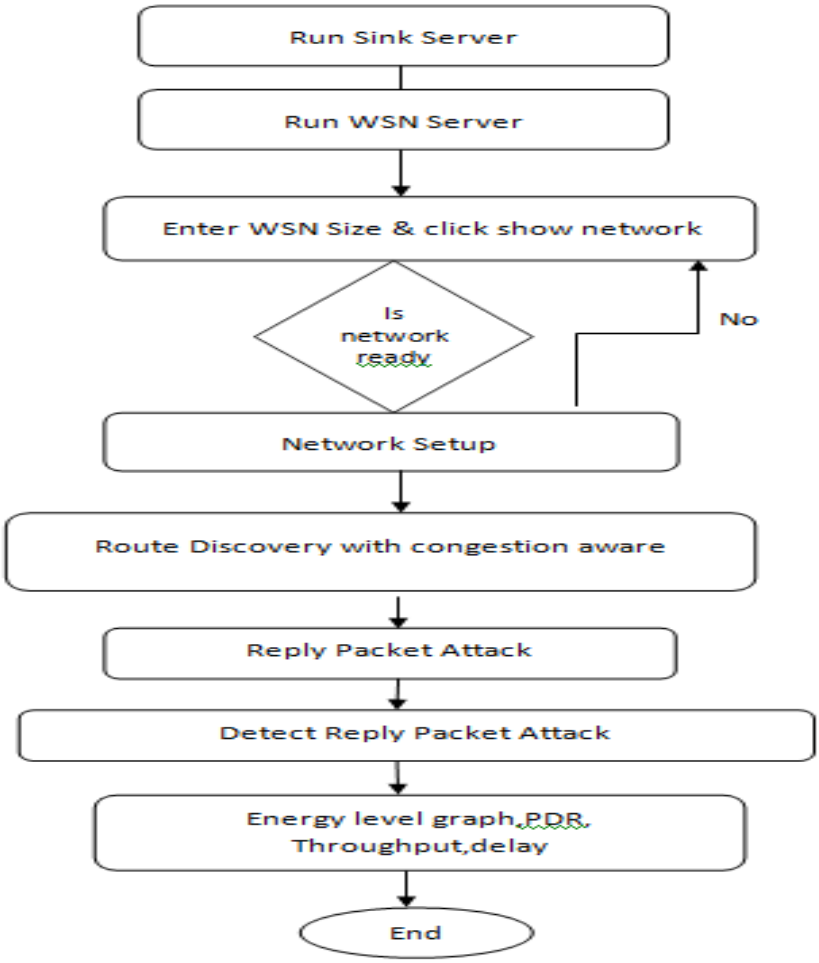

Fig. 5: Activity Data Flow Diagram

RESULTS

First start sinks by double click on ‘run.bat’ file from ‘Sink’ folder to get below screen in Fig. 19.

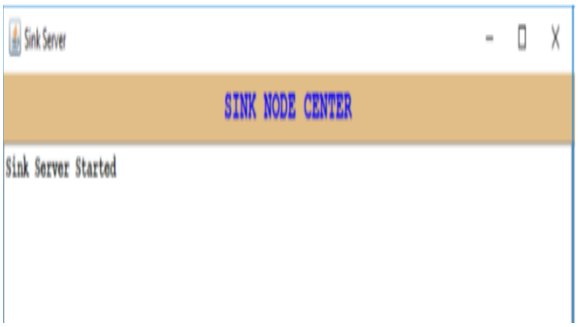

Figure.6. sink server started

Now start WSN simulation by clicking on ‘run.bat’ file from WSN folder.

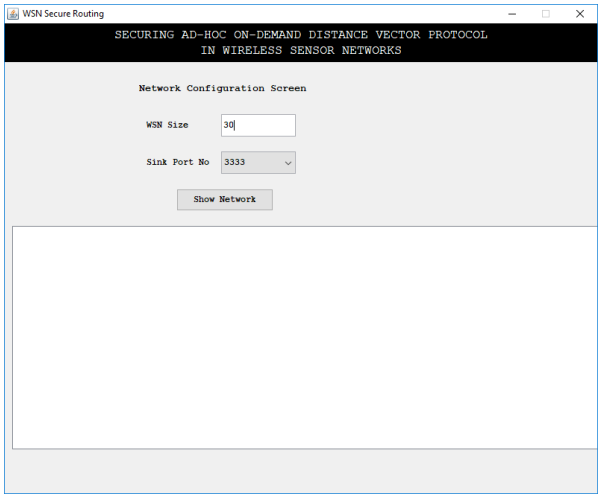

Figure.7. enter size

Enter number of nodes in above screen and press Show Network’ button to get below screen

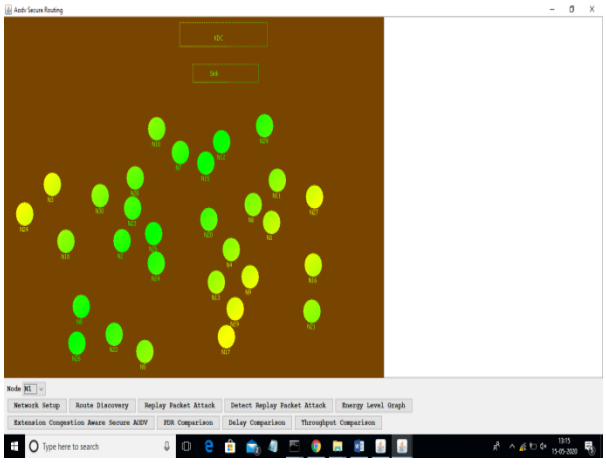

Figure.8. Network view

In above screen run ‘Network Setup, Route Discovery, Replay Packet and Detect Replay packet’ as it in old way. Then click on ‘Extension Congestion Aware Secure Aodv’ button to run AODV in congestion aware mode

Figure.9. Route and discovery of attacks

In above screen propose work choosing N12 to reach sink node without concentrating load on it. Now run same simulation by clicking on ‘Extension Congestion Aware Secure AODV’ button to get below screen

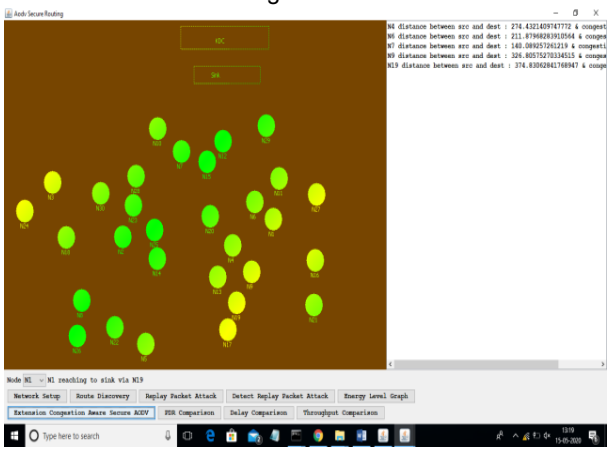

Figure.10. detected less distance and less

In above screen in left side of screen it is seen all neighbors and its distance to sink node with available load on it and application choose path N19 which has less load compare to all. Just scroll text area to right side to see congestion load. Now click on ‘PDR Comparison’ button to get comparison between propose Secure AODV and Extension Congestion Aware technique

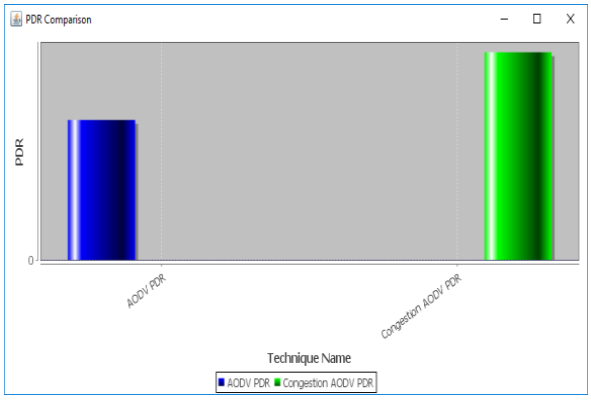

Figure.11. PDR comparison

In above screen x-axis represents technique name and y-axis represents PDR of that technique. Now click on 'Delay Comparison' button to get below graph

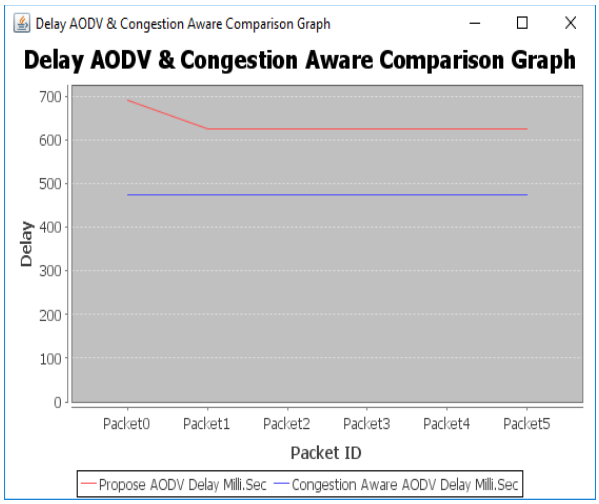

Figure.12. Delay Comparison

In above graph x-axis represents packet id and y-axis represents delay for that packet in milliseconds. Redline refers to propose work and blue line refers to extension congestion aware technique. Now click on 'Throughput Comparison' button to get below comparison graph

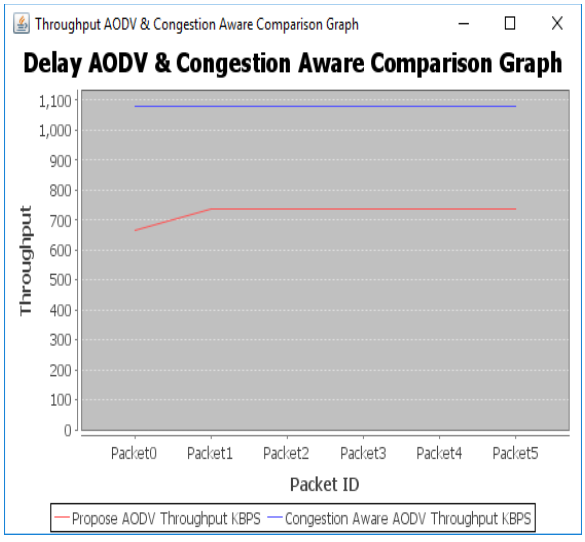

Figure.13. throughput comparison

In above graph x-axis represents packet id and y-axis represents throughput per KBPS for that packet.

Conclusion

Replay attacks inevitably affect vitality stockpiling in WSN Hubs or nodes. They decline leftover vitality and increment traded convention and information messages. Sprout channels can rescue vitality stockpiles in various levels as indicated by how large the WSN is and to what extent the way of transmission is. Clog is a significant issue in versatile impromptu systems prompting bundle misfortune and debasement of the system. Since AODV has no clog control system, the blockage control conventions dependent on AODV with secure filter with replay and bloom filter is clearly mentioned in this paper. The output in the congestion aware and bloom filter-based model in security is successfully implemented on java platform. The results clearly show higher efficiency in terms of energy, PDR, throughput and delay in the wireless sensor network.

References

1. N. AlMansour and S. Alahmadi, "Secure Ad Hoc On-Demand Distance Vector Routing Protocol in WSN," 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, 2018, pp. 1-4, doi: 10.1109/CAIS.2018.8441991.
2. S. Akhdar, "Securing Ad-Hoc On-Demand Distance Vector Protocol in Wireless Sensor Networks: Working with What the Node Can Offer," 2018 International Conference on Computing Sciences and Engineering (ICCSE), Kuwait City, 2018, pp. 1-6, doi: 10.1109/ICCSE1.2018.8374222.
3. P. Papadimitratos and Z. J. Haas, "Secure on-demand distance vector routing in ad hoc networks," IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, 2005., Princeton, NJ, 2005, pp. 168-171, doi: 10.1109/SARNOF.2005.1426537.
4. Ye Tung, M. Alkhatib and Q. S. Rahman, "Security Issues in Ad-Hoc On-Demand Distance Vector Routing (AODV) in Mobile Ad-Hoc Networks," Proceedings of the IEEE SoutheastCon 2006, Memphis, TN, 2006, pp. 339-340, doi: 10.1109/second.2006.1629376.
5. R. S. Mangrulkar and M. Atique, "Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network," 2010 Sixth International conference on Wireless Communication and Sensor Networks, Allahabad, 2010, pp. 1-4, doi: 10.1109/WCSN.2010.5712310.
6. J. T. Kim, J. Kho, C. Lee, D. Lee, C. Bang and G. Lee, "A Safe AODV (Ad Hoc On-Demand Distance Vector) Security Routing Protocol," 2008 International Conference on Convergence and Hybrid Information Technology, Daejeon, 2008, pp. 115-118, doi: 10.1109/ICHIT.2008.289. J. T.
7. Perkins, Charles & Belding, Elizabeth. (1999). Ad-hoc On-Demand Distance Vector Routing. Proc. 2nd IEEE Workshop on Mobile Computing Syst. and Applications (WMCSA '99) (New Orleans, LA. 25. 90-100. 10.1109/MCSA.1999.749281.
8. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey. Computer Networks", 38(4): 393–422.

http://doi.org/10.1016/S1389-1286(01)00302-4, 2002
9. T. Aura, “Strategies against Replay Attacks”. Proceedings of Computer Security Foundations Workshop, 59–68. Rockport, MA: IEEE http://doi.org/10.1109/CSFW.1997.596787, 1997.
10. B. Bloom, “Space/Time Trade-Offs in Hash Coding with Allowable Errors”. ACM Communications, 13(7): 422—426, 1970.
11. A. Broder, and M. Mitzenmacher, “Network Applications of Bloom Filters: A Survey”. In Internet Mathematics 1(4): 485–509. A K Peters.
12. Kumar, Manoj, and Ashish Sharma. "Mining of data stream using “DDenStream” clustering algorithm." 2013 IEEE International Conference in MOOC, Innovation and Technology in Education (MITE). IEEE, 2013.
13. Sharma, Ashish, Anant Ram, and Archit Bansal. "Feature Extraction Mining for Student Performance Analysis." Proceedings of ICETIT 2019. Springer, Cham, 2020. 785-797.
14. Sharma, Ashish, and Dhara Upadhyay. "VDBSCAN Clustering with Map-Reduce Technique." Recent Findings in Intelligent Computing Techniques. Springer, Singapore, 2018. 305-314.
15. Sharma, Ashish, Ashish Sharma, and Anand Singh Jalal. "Distance-based facility location problem for fuzzy demand with simultaneous opening of two facilities." International Journal of Computing Science and Mathematics 9.6 (2018): 590-601.
16. Ram, Anant, et al. "A density-based algorithm for discovering density varied clusters in large spatial databases." International Journal of Computer Applications 3.6 (2010): 1-4.
17. Kulshrestha, Jagrati, and Anant Ram. "An Analytical Study of the Chain Based Data Collection Approaches." 2019 4th International Conference on Information Systems and Computer Networks (ISCON). IEEE, 2019.
18. Verma U., Bhardwaj D., 2020 "Design of Lightweight Authentication Protocol for Fog enabled Internet of Things - A Centralized Authentication Framework", International Journal of Communication Network and Information Security Vol 12, No 2 (2020) pp. 162-167
19. Mr. Rakesh Kumar & Prof. Diwakar Bhardwaj, as their research paper titled, "EBH-DBR Energy Balanced Hybrid Depth Based Routing Protocol for Underwater Wireless Sensor Networks", has been accepted for publication in the World Scientific Journal (SCI Indexed).
20. Varun K L Srivastava, N. Chandra Sekhar Reddy , Dr. Anubha Shrivastava, "An efficient Software Source Code Metrics for Implementing for Software quality analysis", International Journal of Emerging Trends in Engineering Research, Volume 7, No. 9 September 2019.