Cluster based Certificate Blocking Scheme using Improved False Accusation Algorithm

Chetan S Arage[1], K.V.V. Satyanarayana[2]
Department of CSE, Koneru Lakshmaiah Education Foundation
Vaddeswaram, Guntur – 522502, Andhra Pradesh, India

***Abstract*—The aggregation of mobile nodes without the use of a base station is known as Mobile Ad Hoc Networks (MANETS). In nature, the nodes are moving. These networks are not connected and thus subject to security attacks due to their mobility. There are several mechanisms proposed to prevent mishaps while routing of the packets in such networks methods: The methodology outlined in Mobile Ad Hoc Networks to protect against various types of assaults is based on a recent method known as Cooperative Bait Detection Scheme. Its implementation scenario demonstrates that in the event of Sybil assaults, the packet delivery ratio and performance are low. on the network. Our goal is to propose a cluster-based methodology to improve delays, packet delivery ratio, and other performance assessment criteria. Improved Cooperative Bait Detection recommends a disjointed multipath technique to avoid attacks. Until date, the dropped packet delivery ratio has been the key to preventing collaborative and Sybil assaults. In the Hybrid Cooperative Bait Detection Scheme, nodes are verified in two stages: first, on the basis of packet delivery ratio, and then, in the second stage, the exact cause of performance decline is explored to check node behavior. In order to improve security, certifying procedures must be used to clustered networks. For malevolent entities, the false accusation algorithm provided certificate revocation and blocking approaches. An algorithm is proposed that remembers false accusations for a set period of time in order to increase the number of normal nodes in the network and hence improve the system's performance. Results: With the help of NS2 simulation, the clustering approach was evaluated by considering several Sybil-attack network scenarios. When the proposed work is compared to other ways such as Cooperative Bait Detection Scheme, Improve Comparative Bait Detection Scheme, and Hybrid Comparative Bait Detection Scheme, the results show that Packet Delivery Ratio and performance are improved for Sybil attackers over the internet. In conjunction with Certifying authority, the Cluster Head in the network identifies and prevents false complaints. The results of the comparison using several performance parameters reveal that the new strategy outperforms the existing ones. As the number of normal nodes in the system grows, the system will be able to work at its best, preventing various types of attacks.**

Keywords*—*Mobile Ad Hoc Networks; cooperative bait detection scheme; cluster; cluster head; certifying authority; certificate revocation

I. Introduction

The AdHoc Mobile Network is a less dependable wireless network for the infrastructure. [1]. Since the 1980s wireless mobile systems have been in use. We saw their developments in wireless systems of the first, second, and third generations. With the assistance of a centralized support structure like an access point, wireless networks function. These access points help wireless users to maintain connections from one area to the other with the wireless system. The existence of a permanent support structure inhibits wireless solutions' adaptability [2]. So Bluetooth provided a new sort of wireless system called ad hoc mobile networks to develop wireless networks (MANETs).

Mobile Ad Hoc Networks (MANETS) is the aggregation without the base station of mobile nodes. The nodes are moving in nature. Due to its mobility, these networks are not wired yet vulnerable to security assaults. There are several mechanisms proposed to prevent mishaps while routing of the packets in such networks. MANET is free to roam in any direction and consequently regularly changes its connections to other devices. The goal of connecting “everywhere and every time,” mobile Adhoc networks can make true. Wireless ad hoc mobile network is usually shown as Fig. 1.

A. *Misbehaving Nodes in MANETS*

A mobile node might be dubbed a selfish or misbehaving node to gain from other nodes. This node produces its own network connection certificate and attempts to communicate with other genuine network nodes [3]. It also acts like denying or not responding to other nodes to forward data packets to preserve its battery power.

B. *Blocking of Misbehaving Node*

With an unsafe node, secure communications between network nodes are interrupted. MANETS utilizes weighted bunching strategies to construct geography. Hubs inside the organization structure a bunch that is a group head (CH) along with certain group individuals (CM)[4]. Security is the critical need of MANET in light of the versatility of the hubs [3].

Fig. 2 shows the MANET working using the clustering approach. For overall study it finds that there is the number of activities in mobile Adhoc network but due to its ad-hoc nature number of unknown activity can occur which causes the problem in the network that indirectly affects the working and throughput. So it is expected to protect the adhoc network by detecting the unknown activity so can improve the performance without affecting the network communication.

The following section gives a detailed overview of each attack with the proposed approach to detect the malicious activity.

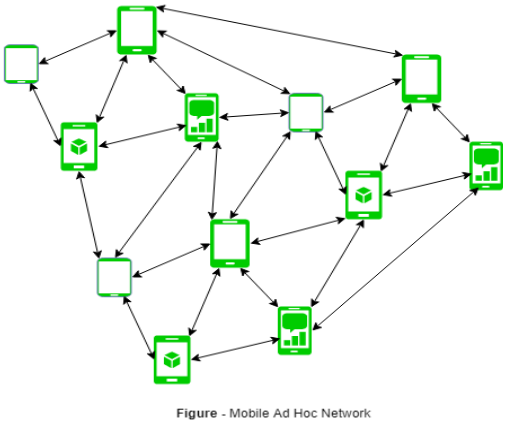
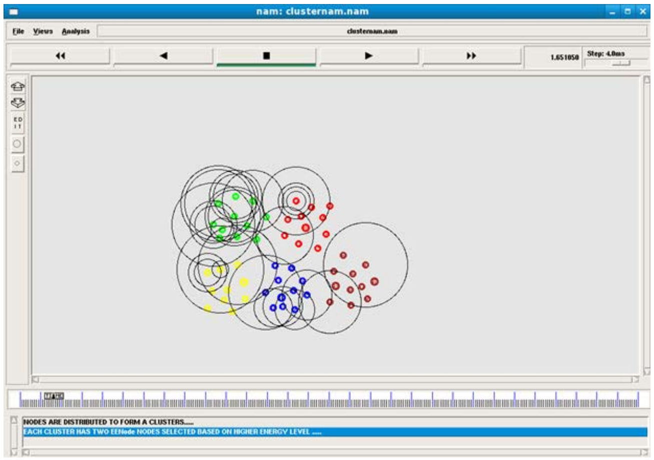


Fig. 1. MANET Environment.



NODES ARE DISTRIBUTED TO FORM A CLUSTERS.....
EACH CLUSTER HAS TWO EENode NODES SELECTED BASED ON HIGHER ENERGY LEVEL .....

Fig. 2. MANET Working with Clustering.

Section II gives the details of MANET attacks and related works. Section III discusses the proposed approach use in-network to secure communication between the nodes. Section IV shows the simulation outcome followed by the conclusion and future scope.

II. Related Work and Classification

This session gives a details overview of attack and review in mobile adhoc network.

A. *Data Traffic Attack*

DATA traffic attacks either in nodes that discard data packets or in data packets that hold forwarding. A couple of forms of assaults are picked for dropping victim packets, while others drop them altogether independent of sender nodes. This can increase service end to end and decrease service value. It can also lead to considerable loss of data. Moreover, few nodes might be completely out of the way save for a redundant path near the irregular node.

B. *Control Traffic Attack*

MANET is naturally susceptible to attack because of its primary features, like open medium, conveyed hubs, self-governance for network investment (can connection and leave the organization as indicated by its will), absence of focal position (which can force net wellbeing on the organization), disseminated coordination and communitarian activities [6].Because of these reasons, the present routing protocols in MANET cannot be used. MANET has many different routing protocols with their individual characteristics and set of legislation [7]. The DYMO is a fast light routing technology created for Multi-Hop networks that depend upon the cooperation of each individual Node in defining the genuine routing table. But they all rely on confidence in networked nodes [14]. The first stage for a successful attack is that the node is a network component. Since there are no constraints on network membership, the hostile node can be connected to and disrupted by capturing routing tables or by dodging lawful routes.

In addition, if the node can determine itself as the quickest route to any target, it may spy on the network using unsafe routing protocols. That is why the protocol for routing must be maximally safeguarded [17]. Similar assaults are not CONTROL assaults and may be mitigated in physical security mechanisms, especially for jamming assaults.

A recent method known as Cooperative Bait Detection Scheme is the basis of the methodology described in [3] Mobile Ad Hoc Networks to defend against various forms of assaults. Its implementation scenario reveals that the delivery ratio and performance of the packet are low in the event of Sybil assaults on the network Improved Cooperative Bait Detection suggests disjoint multipath strategy to prevent assaults. Dropped Packet delivery ratio is the key for implementation to prevent collaborative and Sybil assaults till now.

In Hybrid Cooperative Bait Detection Scheme two stage verification of nodes is done where node which found malicious in first stage on the basis of packet delivery ratio, later stage exact cause of performance drop is investigated to check behavior of the node [3].

III. Proposed Work

The below session explain the proposed work use in the simulation approach with malicious activity detection to improve the throughput of the overall network.

It is required to apply certifying mechanisms to clustered networks so as to enhance security measures.

Our goal is to propose a cluster-based methodology to improve delays, packet delivery ratio, and other performance assessment criteria.

The fundamental goal of our proposed work is to combine a cluster-based certificate blocking mechanism with a better false accusation algorithm, which will be discussed later in this section.

Therefore, we updated the CBDS method with the proposed approach to the clustering system. The number of hops of all nodes from the destination is considered [22]. The node receives the packet and only transfers it from that dedicated path in accordance with the CBDS scheme, otherwise, the packet will be discarded. As explained earlier this is carried out before clustering is done by integrating the CBDS algorithm with the proposed false accusation algorithm.

A. Algorithm Design

Assumptions and Abbreviations

CA=Certifying authority

CH= Cluster Head

WL= Warned List

BL= Blocked List

CH=Cluster Head

NN = Number of Nodes

SNi = Specific Node,

SCk = Specific Cluster,

MAX = Number of maximum nodes per cluster,

PD = Packet Data,

NBi = Buffer of Specific Node,

SNTCi = Specific node's trust counter (Initially set to 0 for each node),

SNTSi = Specific node's trust status (Initially set to 'F' for each node)

TV = Threshold Value (Set default is 0.8)

k = Used for Cluster Number

count = Used to count number of nodes in cluster

Algorithm

```
Initialize
k = 0
count = 0
Step 1: Cluster formation
for i = 1 to NN
{
Find out degree of each node ();
Find out power status of each node ();
}
while (making cluster by putting every node in to any one cluster)
   {
   if (SNi = = max (degree of node and power status of node))
        {
           Add SNi into SCi
           Set count = count +1
        }
   if (count > MAX)
        {
              k++
              Set count =0
           }
      }
Step 2: Detection of suspected nodes

while (SNTCi < TV)
{
     if ( SNi sends accusation message against node M = True)
        {
          CA updates WL and BL
        }
     else
         {
          CH sends recovery packet to CA
          CA broadcast this information
         SNTCi = SNTCi + 0.2
         }
  }
Step 3: Process for suspected nodes
Send Testing packet data RREQ to the node with TTL=1
if (receives response)
  {
      if (SNTCi  < TV )
             Set SNTSi as 'F'
   }
else
     {
      Set SNTSi as 'D'
      Go to step 4
  }
Step 4: Detection of false accusation ();
Step 5: Send accusation message for time t
```

False accusation algorithm proposed certificate revocation and blocking techniques for malicious entities. An algorithm proposed remembers false accusation for certain amount of time to achieve increased number of normal nodes in the network and hence improves performance of the system.

B. Environment used in Proposed Approach

The network environments of 1000 m * 1000 m with various numbers of nodes are seen in Table I below. In addition, the suggested phenomenon was tested against malevolent situations in which the intruders were infected by a variety of legal nodes. In existence, the CUs became movable, where they could at any moment break from their network or combine. In addition, 802.11 was the underlying MAC layer standard, although the routers' transmission range was restricted to 250 m [14]. To quantify the protection, during the handoff and communication process, the malevolent nodes or CUs were inserted into the environment using the probability distribution.

TABLE I. PARAMETERS USED IN AD HOC NETWORK FOR SIMULATION

Simulation Time Number of nodes	1000 seconds 50
Number of Malicious Nodes	0,5,10,15,20 (Scenario)
Network Size	1000 m X 1000 m
Transmission Range Maximum Speed	250 m 1 m/s – 10 m/s
Mobility Model Traffic Type	Random Way Point CBR
Number of Source Destination Pairs	30 %
IFQ Size Channel Bandwidth	NS2 Default 2 Mbps

C. Parameters

In our experimentation, there are multiple inputs and output attributes. The input features are the number of nodes and the time of arrival. The proposed algorithm would follow all scheduling requirements such as overall performance, packet transmission rate, reduced return time, minimum waiting time, minimum power usage, and minimum end-to-end delay in multiple cases of arrival time [12]. The algorithm will then be implemented to test the proposed process. In each case of our experiment for the assessment of results, we consider different performance measurements; some of the normal performance parameters are,

1) Throughput: It is a network computing efficiency parameter for the supply of packets of data from the source to the destination. This attribute reflects network performance and is crucial.

2) End to end delay: It is defined as the total amount of all plausible delays made due to buffering when the task of the route discovery process is ongoing and completed.

3) Packet delivery ratio: it gives the ratio of the total amount of packets delivered to the total amount of packets lost. This parameter signifies the efficiency of transmission.

Evaluate the proposed approach, namely improve energy-efficient resource allocation (IEERA) in cognitive radio networks using clustering. The other variables that influence this are transfer & propagation delays, transmission delays, interface queue, etc. output in various network scenarios in terms of node movement rate, multicast group size, resource assignment group number [13]. The number of multi-cast destinations is calculated between 5 and 20 radio nodes in this simulation. The amount of traffic is 10 packets per second.

D. Energy Efficiency

Energy performance is one of the key problems in the architecture of wireless sensor node MAC protocol. In MAC-layer protocols, diverse sources contribute to energy conservation. The first energy waste source is a crash, triggered by two or more sensor nodes concurrently transmitting. The need to re-transmit a broken packet increases the consumption of electricity. The second explanation for energy depletion is lazy listening. When you hear traffic that is not being sent, a sensor node enters this mode. In many sensor network implementations, this energy-consuming silent channel monitoring can be high. The third source of energy waste is overheard when a sensor node collects packets for other nodes.

Energy Efficiency= Energy utilized by node / Total energy of the node

E. Congestion Control

Congestion takes place when traffic approaches the combined or total potential of the underlying networks. Therefore, more modern methods to eliminate, track and overcome congestion must be built-in special con-side rations. When designing certain strategies for maximal performance, the finite resources of the WSN need to be considered. Diverse techniques, including protocols for routing aided by congestion detection and control mechanisms and complex protocols for congestion control, have been adopted in the last few years.

IV. SIMULATION AND RESULTS

Cluster-based bait detection system performance review of the proposed system model in the Ad hoc Network is tested and contrasted with Boost DSR, CBDS, and HCBDS routing system based on some parameters successful the stable routing protocol applied in the presence of Sybil attack.

The clustering strategy with the help of NS2 simulation and assessed by taking into consideration various Sybil-attack network situations. The outcomes of the planned work is compared with Cooperative Bait Detection Scheme), Improve Comparative bait detection Scheme & Hybrid Comparative bait detection Scheme approaches indicate that PDRs & performance are being enhanced for Sybil attackers over the internet as compared to other existing approaches. Cluster Head in the network detects and prevents fake allegations in association with Certifying authority. The comparative result with different performance parameters shows that the proposed approach gives a better outcome as compare to the existing ones. As the number of normal nodes in the system is increased the system is able to perform at its best with achievable prevention to different kind of assaults.

Performance Analysis of proposed system model namely Cluster basted is evaluated and compared with conventional DSR and CBDS based on parameters like false positives, detection rate, energy consumption, packet loss rate. Following is some Performance analysis of cluster-based approach with proper procedure.

A. *False Positives*

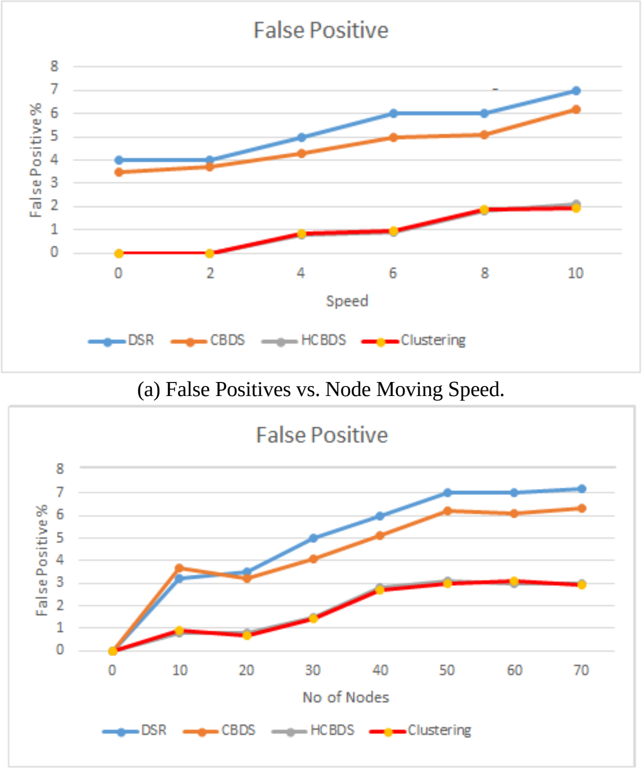
The False Positives Sum is the ratio of legal nodes considered unsafe to the total legal node numbers. We contrasted the architecture proposed with the DSR, CBDS, HCBDS system in the terminology of positives that are false, this time gripping all the frameworks together with our model of optimization, and incorporating nodes that are malicious into the network [12]. The incidence of false positives with increased speed of node movement is shown in Fig. 3. From the diagrammatic representation, it is clear that the rate of false positives decreases to a far bigger degree in our Cluster-based system compared to the other scheme. In reality, our proposed methodology better analyses the overall possible cause of an event of packet drop, and then a decision is made on the trustworthiness of the node. Overall, the statistic indicates that with an increase in growing node speed the false positive rate increases. On similar lines, Representation indicates a false positive rate along with the growing density of the node in the network, keeping the moving speed is 4 m / sec at the node is rigid. With an increased count of a node in the architecture, the source/destination number pairs are also increasing, because due to collisions, more packets are lost in the network. The number of false positives in the Cluster-based scheme is smaller relative to numerous other schemes, which considers every packet drop as an activity that is malicious [28], because the frequency of each packet drop is measured before making any judgment on the behavior of nodes and its multipath strategies.

In Fig. 3 shows the false Positives versus node Moving Speed with moving velocity and thickness on bogus positives where the x-pivot addresses the no of hubs use in-network and the y-hub addresses the False Positives rate.

B. *Detection Rate*

The rate of detection with rising moving nodes under the Cluster-based scheme and the other device is shown in Fig. 2. In our Cluster-based system, the detection rate is higher, as every decision is unbiased. The detection rate is the number of true malicious nodes found in the scheme relative to the total number of malicious nodes. The other plan considers every parcel drop as malevolent and the related hub is viewed as malignant and consequently more real hubs are vindictive. As the insights show, the recognition rate for our Cluster-based plan is higher than for the other plan. Moreover, the identification rate with developing hub thickness is displayed in Fig. 2. The quantity of information associations inside the organization is additionally developing with the expanding hub thickness, which implies that more parcels are dropped on the organization because of crashes. The other scheme considers packet drops to be misbehavior of valid nodes. Therefore the detection rate in our Cluster-based scheme is higher again than in other schemes, as shown in the figure.

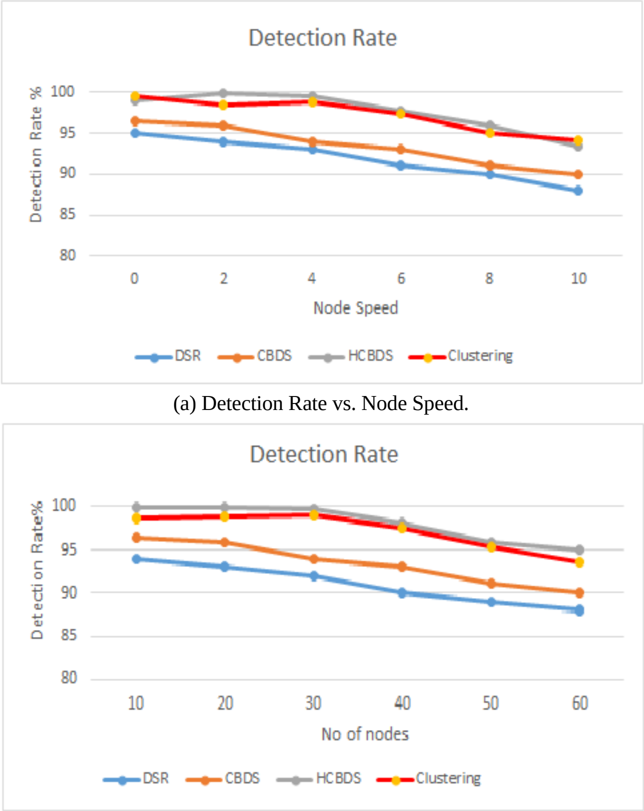
In Fig. 4 shows the Detection Rate vs. Node Speed with moving velocity and thickness on identification rate where the x-pivot addresses the no of hubs use in-network and the y-hub addresses the Detection rate.



(a) False Positives vs. Node Moving Speed.

(b) False Positives vs. No Node Density.

Fig. 3. Effect of Node Moving Speed and Density on False Positives.



(a) Detection Rate vs. Node Speed.

(b) Detection Rate vs. Node Density.

Fig. 4. Effect of Node Moving Speed and Density on Detection Rate.

C. Energy Consumption

Fig. 5 shows the energy consumed under the Cluster-based system and CBDS schemes at rising node speeds. The goal of this experiment is to show that the total costs of processing and communication in the Cluster-based scheme are higher compared with the method i.e. the CBDS and other schemes. Packet transmission and receipt absorb most node resources. There is a novel energy-efficient secure routing protocol for the ad-hoc network with a Mobile sink [26]. Our Cluster-based plan doesn't build the quantity of traded messages; rather it utilizes existing directing bundles to trade data like line status and association status (already required according to routing Protocol standards). In addition, the data path continues to convey true malicious nodes.

D. Packet Loss Rate

In the cluster-based system and CBDS schema, the packet loss rate is shown in Fig. 6. The packet loss rate in our cluster system is less than in the CBDS scheme, as is seen in the figure. In reality, in the cluster-based routing path system more trustworthy nodes are chosen which leads to reduced packet losses and greater packet delivery ratios. For the CBDS & Other systems, genuine node isolation is possible, which leads to a greater drop in packets since transmission nodes to the destination are not available. In addition, the data path remains true malicious nodes, which provide them more possibilities of dropping vital data packets.

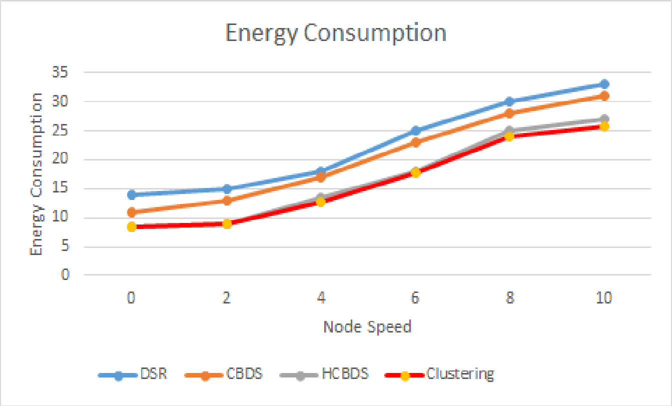


Fig. 5. Energy Consumption.

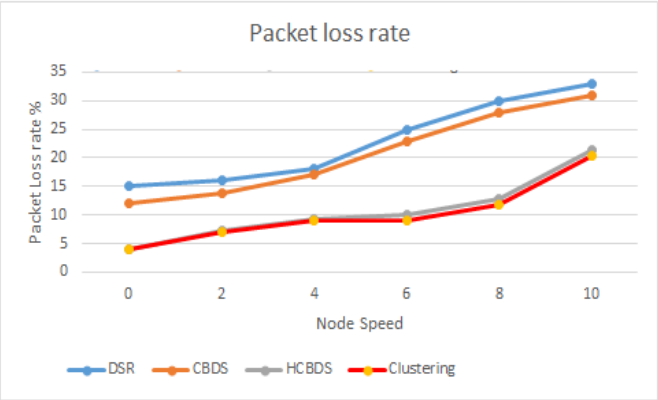


Fig. 6. Packet Loss Rate.

E. Packet Delivery Ratio (PDR)

PDR of Conventional DSR routing protocol. PDR is the presence of Sybil attack, partially secure CBDS routing protocol and proposed Cluster-based System, is shown in Fig. 7. The percentage data loss in DSR & CBDS under Sybil Attack is increased more than the Cluster-based routing protocol in all scenarios.

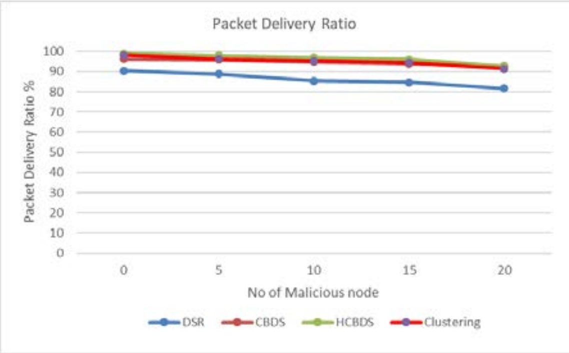


Fig. 7. Performance Analysis of Packet Delivery Ratio using DSR, CBDS, HCBDS & Clustering.

F. End to End Delay

The end-to-end delay performance of the conventional DSR, CBDS, HCBDS & clustering is the results are shown in Fig. 8. The CBDS, HCBDS producing over average end-to-end delay compared with clustering produces. From the results, it concludes that the model is flooding a minimum number of delays as compared to other.

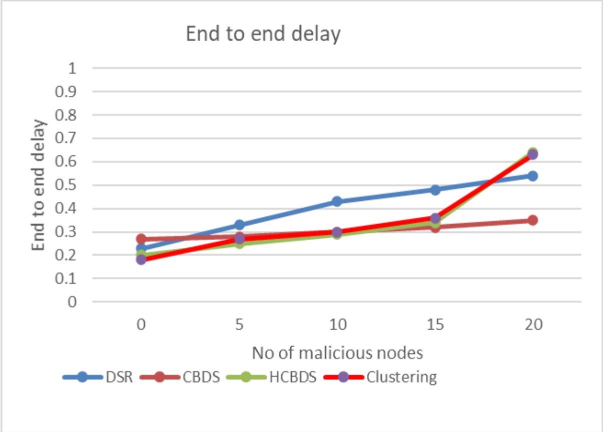


Fig. 8. Performance Analysis of End to End Delay using DSR, CBDS, HCBDS & Clustering.

V. Conclusion and Future Work

Among other things, Sybil assaults are known as the most dangerous Adhoc network attacks. While several mechanisms exist for protecting Adhoc networks from such attacks, there are significant limitations and several drawbacks in the conventional approach. In addition, during the path discovery process, DSR does not detect malicious nodes and hence cannot send all data packets to the target during Sybil attacks. Many conventional approaches are inefficient to detect malicious activity. In addition, the delivery ratio of packets (PDR) under these attacks may decrease with an increase of malicious nodes. Therefore, a new Clustering mechanism was proposed to protect ad hoc networks.

An advanced version of DSR with Clustering is first used to find and protect the malicious nodes that lead to attacks when a network is built using an NS-2 simulator. Additional encryption was done twice to boost security. It guarantees confidentiality to ahead and back. Whenever topology changes, all authenticated neighbors obtain the new neighborhood key and will be supported. In conclusion, all of these mechanisms prevent attacks of Sybil, and the proven growth in performance and an improved Packet Delivery Ratio are especially worthy of attention.

By looking at the result, the proposed system showed improved performance in terms of packet delivery ratio and output compared to the CBDS, HCBDS processes. This proposed work increases the number of normal nodes in the network and hence improves the performance. In the future, we can focus on the detection of different attacks with their performance analysis.

In future work we intend to investigate:

1) Varying density evaluation in the clustered network.

2) Other parameters of packet losses like MAC layer information.

3) Performance of our method under different security threats in the mobile ad-hoc network.

References

[1] H L Bhavyashree ,Nagarathna C R , Anusha Preetham,Priyanka R “Modified cluster based certificate blocking of misbehaving nodes in MANETs” International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering March 2019.

[2] Chetan S Arage, K. V. V. Satyanarayana, “An experimental analysis on various techniques for malicious node detection in MANET”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.

[3] Arage Chetan S, Satyanarayana K V V,“Novel Routing Protocol for Secure Data Transmission in Wireless Ad Hoc Networks”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-4S2 March, 2019.

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ‘‘VANet security challenges and solutions: A survey,’’ Veh. Commun., vol. 7, pp. 7–20, Jan. 2017.

[5] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, ‘‘Overcoming the key challenges to establishing vehicular communication: Is SDN the answer,’’ IEEE Commun. Mag., vol. 55, no. 7, pp. 128–134, Jul. 2017.

[6] I. Ahmad, R. M. Noor, I. Ali, M. Imran, and A. Vasilakos, ‘‘Characterizing the role of vehicular cloud computing in road traffic management,’’ Int. J. Distrib. Sensor Netw., vol. 13, no. 5, 2017, Art. no. 1550147717708728.

[7] Muhammad saleem khan, daniele midi, majidiqbal khan, elisabertino, “fine-grained analysis of packet loss in manets”, 2169-3536 2017 ieee.

[8] I. Ahmad, U. Ashraf, and A. Ghafoor, ‘‘A comparative QoS survey of mobile ad hoc network routing protocols,’’ J. Chin. Inst. Eng., vol. 39, no. 5, pp. 585–592, 2016.

[9] L. Li and G. Lee, ‘‘DDoS attack detection and wavelets,’’ Telecommun. Syst., vol. 28, nos. 3–4, pp. 435–451, 2005.

[10] C. Buragohain, M. J. Kalita, S. Singh, and D. K. Bhattacharyya, ‘‘Anomaly based DDoS attack detection,’’ Int. J. Comput. Appl., vol. 123, no. 17, 2015.

[11] S. S. Manvi and S. Tangade, ‘‘A survey on authentication schemes in VANETs for secured communication,’’ Veh. Commun., vol. 9, pp. 19–30, Jul. 2017.

[12] Srinivasa Rao, Y., & Hussain, M. A. (2018). Dynamic MAC protocol to enhancing the quality of real time traffic in MANET using network load adaptation. Journal of Advanced Research in Dynamical and Control Systems, 10(7 Special Issue), 1612-1617.

[13] Suma, P., & Hussain, M. A. (2018). Secure and effective random paths selection (SERPS) algorithm for security in MANETs. International Journal of Engineering and Technology(UAE), 7(2), 134-138. doi:10.14419/ijet.v7i2.8.10345.

[14] A. Sinha and S. K. Mishra, ‘‘Preventing VANET from DOS & DDOS attack,’’ Int. J. Eng. Trends Technol., vol. 4, no. 10, pp. 4373–4376, 2013.

[15] Boddu, N., Vatambeti, R., &Bobba, V. (2017). Achieving energy efficiency and increasing the network life time in MANET through fault tolerant multi-path routing. International Journal of Intelligent Engineering and Systems, 10(3), 166-172. doi:10.22266/ijies2017.0630.18.

[16] Kolagani, P., Aditya, K., Venkatesh, N., & Kiran, K. V. D. (2017). Multi cross protocol with hybrid topography control for manets. Journal of Theoretical and Applied Information Technology, 95(3), 457-467.

[17] K. Verma and H. Hasbullah, ‘‘Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET,’’ Secur. Commun. Netw., vol. 8, pp. 864–878, Mar. 2015.

[18] Jun- zaho sun, “Mobile Ad hoc Networking: An essential technology for pervasive computing”, Machine Vision and Media Processing,2000.

[19] Tarunpreet Bhatia , A.K. Verma , “ Security Issues in Manet: A Survey on Attacks and Defense Mechanisms ,“ International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, pages 1-4,June 2013.

[20] Kang, N., Shakshuki, E and Sheltami, T. , “Detecting Misbehaving Nodes in MANETs”, In Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pages 216-222, 2010.

[21] Mainak Chatterjee, Sajal K. Das and Damla Turgut, “WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks,” Center for Research in Wireless Mobility and Networking (CReWMaN) Cluster Computing 5, pages 193–204, 2002.

[22] P.Sakarindr and N. Ansari, “Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks,” IEEE Wireless Comm., vol. 14,no. 5, pages 8-20, Oct. 2007.

[23] Nirwan Ansari, Wei Liu and Hiroki Nishiyama, “Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks,” IEEE transactions on parallel and distributed systems, vol. 24, no. 2, pages 1-4, February 2013.

[24] Seung Yi, Robin Kravets, “MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks,” University of Illinois at Urbana Champaign Urbana, pages 1-6, 2000.

[25] Dr. Shaveta Ran1, Dr. Paramjeet Singh, Raman Preet, “Reviewing MANETs & Configurations of Certification Authority (CA) for node Authentication,” International Journal of Computer Science and Information Technologies, Vol. 4 (6), pages 974-978, 2013.

[26] Kavitha. V, Ananthakumaran. S, “Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink,” International Journal of Peer-to-Peer Networking and Applications, October, 2018.

[27] Ananthakumaran. S, Sathishkumar. M, Bhavani. R, Ravinder Reddy. R, “Prevention of Routing Attacks using Trust-Based Multipath Protocol,” International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, No. 3, pp. 4022-4029, May-June, 2020.

[28] Shivaprasad More, Udaykumar Naik “A Novel Technique in Multihop Environment for Efficient Emergency Message Dissemination and Lossless Video Transmission in VANETS” JCIN IEEE Journal- Volume 3, Issue 3 September 2018.

[29] Shivaprasad More, Udaykumar Naik “Optimal Multipath routing for video transmission in VANETs” Wireless Personal Communication (WPC) , https://doi.org/10.1007/s11277-020-07740-1.