

ITC 1/50 Information Technology and Control Vol. 50 / No. 1 / 2021 pp. 45-54 DOI 10.5755/j01.itc.50.1.25002	A Hybrid Efficient Distributed Clustering Algorithm Based Intrusion Detection System to Enhance Security in MANET	
	Received 2020/01/02	Accepted after revision 2021/02/17
	 http://dx.doi.org/10.5755/j01.itc.50.1.25002	

HOW TO CITE: Rathish, C. R., Karpagavadivu, K., Sindhuja, P., Kousalya, A. (2021). A Hybrid Efficient Distributed Clustering Algorithm Based Intrusion Detection System to Enhance Security in MANET. *Information Technology and Control*, 50(1), 45-54. <https://doi.org/10.5755/j01.itc.50.1.25002>

A Hybrid Efficient Distributed Clustering Algorithm Based Intrusion Detection System to Enhance Security in MANET

C. R. Rathish

Department of Electronics and Communication Engineering; United Institute of Technology; Coimbatore, India;
e-mail: r.rathish87@gmail.com

K. Karpagavadivu

Department of Computer Science Engineering; Dr. N. G. P. Institute of Technology; Coimbatore, India;
e-mail: karpagavadivu@drngpit.ac.in

P. Sindhuja

Department of Computer Science Engineering; United Institute of Technology; Coimbatore, India;
e-mail: sindhujaphd@gmail.com

A. Kousalya

Department of Information and Technology; Sri Krishna College of Engineering and Technology; Coimbatore, India; e-mail: kousivetri@gmail.com

Corresponding author: r.rathish87@gmail.com

MANET plays a key role in the contemporary improvements in technology and services that dynamically build up the network connection bringing about a variation in network topology. If any malevolent activity inside the network otherwise in the system occurs, it is monitored by software application or device called Intrusion or Invader Detection System (IDS). The power utilization is more in MANET as the IDS needs to be active for the whole time on each node. Considering this, we have designed a clustering-based proposal for Ad-hoc networks. To lower the communication overhead, the CH (Cluster Head) detection is called upon for establishing the path Weighted Clustering Algorithm (DCA) that is utilized to construct path. The proposed Distributed Clustering Algorithm dependent Invader Detection System (DCAIDS) is designed to reduce the overall delay. The intruder attacks are identified by IDS and that particular nodes are detached from the cluster. When the particular target node receives the packets, it acknowledges its reception by sending RREP message so that the sender can send the intended data packets thereafter. Thus, an efficient and delay tolerant path is established which in turn intensifies the certainty of MANET.

KEYWORDS: MANET, IDS, DCA, Route Reply, Communication overhead.

1. Introduction

Ad-hoc is a regionalized wireless network. Ad-hoc network does not depend on an already built infrastructure, i.e., in several kinds of networks (wired) we reckon on routers and in other type (wireless network) we rely on access point. Alternatively, every individual node inside the network takes part in the procedure of routing by passing the data to some other nodes and so the discretion of node that forwards the information is made dynamically contingent on the connectivity of network. Mobile Ad-hoc Network (MANET) is employed in several places such as emergency service, military communication and environmental monitoring [20]. It is also utilized to provide secure communication in Android smart devices through cloud computing [1, 2]. MANET furnishes distinctive and novel services as these networks are wholly dispersed. In MANET, more energy is utilized for creating and maintaining a cluster. Hence, to reduce this energy utilization during data transfer, CEEES algorithm was implemented that makes use of the LEACH concept [22].

To furnish safety in MANET is not an easy chore because of the built-in attributes of MANET. Moreover, providing security elucidation for a wired network which is fixed is not easy to adapt [3, 14]. One of the ways to provide certainty is by implementing Invader Detection System. This system determines the actuality of intrusion in the particular network in use to fulfil the security demands [18, 19].

The nodes detects the actuality of intrusions and that has been further assigned into two techniques, name-

ly, (1.) Signature-based, and (2.) Anomaly-based intrusion detection. In signature-based invader detection, nodes notify about the perception of signature of attacks. Anomaly-based invader detection is different from signature-based detection. It involves searching of anomalous behavior or events [15, 17]. In the proposed work we are focusing on network-based anomaly detection. It will detect the dribble of information carrying packets and dynamic modifications in the routing table. In almost all the existing proposals IDS needs to run for the whole time in that network [16].

The prime focus of our project is to lessen the on-time of IDS because it leads the way to increased power utilization. Therefore, we are approaching the development of cluster to lessen the IDS active time. Clusters are maintained when data is to be forwarded. The formation of clusters using distributed clustering proposal for routing purpose increases the throughput efficiently and in addition the energy utilization will be plummeted.

Considering all these issues the proposed design – DCAIDS is presented. It provides power optimization by eliminating the requisite for the invader detection system to remain active for the whole time. Instead of that, clusters are formed which could detect the actuality of malevolent nodes in that network which leads to less energy usage and efficiency in transmission.

MANET covers wide area of application and one such important use is in vehicular ad-hoc network (VANET). VANET is a self-configuration network

of monitoring vehicles where the movements of vehicles are restricted by the traffic regulations [7, 28]. Here vehicles are the nodes. Road safeties, traffic efficiency and convenience are improved tremendously by VANET Technology.

2. Related Work

In this segment, we have explored the various initiatives taken to improvise the procedure of invader detection in MANET. We have highlighted the various existing works of IDS in MANET depending on reduction in energy consumption.

Varshney et al. [27] presented a system to enlarge the network performances and security level. They provided an inquiry on watchdog mechanism for routing misconduct in MANET. The watchdog continuously monitors for the actuality of black holes in that network and if suppose an intruder is detected it informs its presence to the sender node and also suggests a new and efficient path for sending the data. Thus, it reduces the packet drip rate but at times watchdog mechanism fails to discover the malicious activities in the actuality of receiver collision along with restricted transmission thus leading the way towards the negligence of the entire system to provide security together with the proportion of packet delivery.

Gracy and Sakthivel [11] proposed a technique to avoid intrusion assault in MANET with the aid of Fuzzy based clustering algorithm. They designed a system which provides two-way intrusion detection. The actuality of malevolent nodes is detected which discovers the anomaly and hence the misuse of the information could be avoided. Thus, it enhances the certainty of data and also enlarges the allegiance of that network. However, it suffers from the drawback that new intruder attacks in WSN cannot be identified and thus leads to the negligence of the overall system.

Balakrishnan et al. [5] presented an approach termed TWOACK to vanquish the various problems in WSN. This scheme helps to detect malicious activity by acknowledging each packet which has been transferred for every three successive nodes starting from the sender to the target. The TWOACK method resolves the problems of collision during reception and restricted transmission power. Owing to the packet acknowledgement process, it utilizes more time thus increasing

the battery power utilization and the network overhead. AACK [25] is like TWOACK, it gives an end-to-end packet acknowledgement, hence both TWOACK and AACK schemes depend upon the acknowledged packet from receiver. In some scenarios, the malevolent nodes send the forged acknowledgement to the sender thereby increasing the practicability of packets drop. Therefore, it is strenuous to analyze whether the acknowledged packets are valid or invalid.

Khalil et al. [13] designed a protocol to provide local monitoring in an effective way. Some special nodes termed as guard nodes were used in SLAM protocol. These nodes were utilized to locally monitor routing inside a network. These nodes extant in inactive mode in the network, when communication is to take place, node awakes the nodes acting as guards before initiating the communication process. SLAM protocol focuses to lower the transmission duration and the guards continues to remain awake for monitoring malicious activity.

Hai and Huh [12] presented an approach in which the procedure of monitoring the node is performed by special monitoring agents called the invader detection agents. Here, agents are none but the monitoring nodes that repeatedly keep checking their neighbors for any malevolent activity. The detection agent helps to monitor packets and sends alert packets to cluster heads. The detection agent gets activated only when the nodes have trust value above the required level. Thus, the neighbors and malevolent nodes inside the cluster are analyzed for small trust database. However, numerous nodes are present inside a network and while transmission there exists a possibility that too many alert packets might get transferred to the CHs which could result in congestion inside the network. Thus, this method is not efficient for smooth transmission.

Elhadi et al. [10] designed an invader perception system for Ad-hoc networks contingent with the acknowledgement packets. EAACK procedure is categorized into three segments i.e., (1.) ACK, (2.) Secure ACK and (3.) MRA (Misbehavior Report Authentication). In the presented method, the sender is required to sign digitally all the packets that are acknowledged which are later substantiated by its receiver. With a view to lessen the time for which the IDS remain active, a feasible model was proposed which utilizes the cooperation among the IDS and the neighborhood node. By utilizing MRA the receiver could find out

whether the misbehavior node report furnished by the sender is valid or not by cross verifying in its own database and in case the report is found invalid then the particular node which has sent this report is observed as malicious node and detached from the communication process.

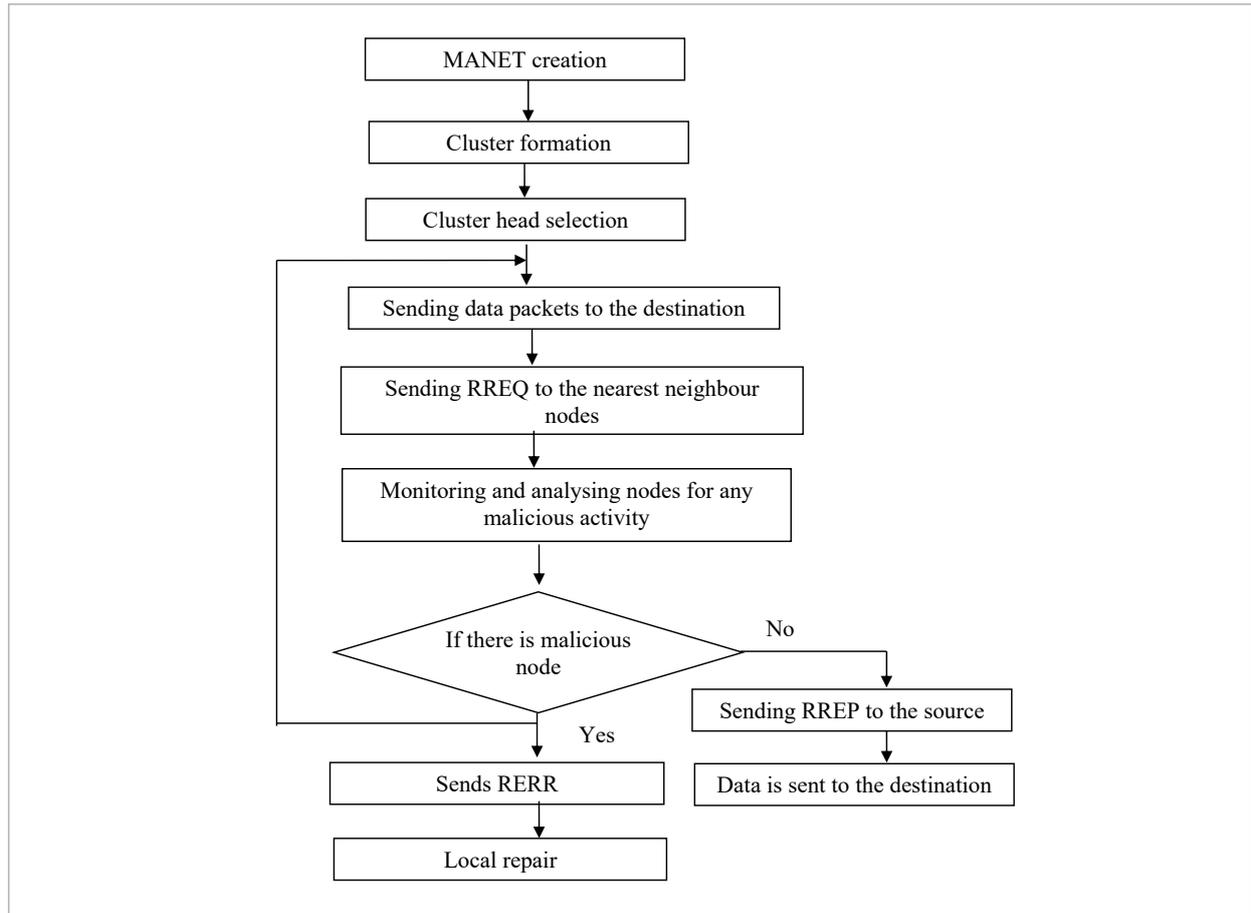
Basant et al. [6] presented a system that utilizes hybrid IDS technique and also an election process for the discretion of cluster leader. Here the CH helps to recognize the actuality of intrusion whereas hybrid IDS which contains two modules, namely, the lightweight and the heavyweight, is utilized to discern the invader assaults. Initially, only the lightweight module will be energized, whereas, the heavyweight component will be actuated only when the lightweight module fails to continue cooperation between the CH and the nodes.

3. An Overview of the System Design

Numerous protocols for routing are already there in existence and each has their own strengths and drawbacks [4]. There are algorithms that provide cost efficient routing by reducing the delay and energy utilization and aid in holding the nodes inside a cluster for as long as possible [24].

Some provide good reliability, packet transmission rate, network lifetime, power efficiency, throughput and the like but nevertheless they suffer from several issues such as security, network overhead, delay, several kinds of assault by the invaders and so on. These issues influence the production of the overall network. Hence, it is important to design a system which deals with all these issues. Therefore, considering

Figure 1
System Flow



this we have designed a system which reduces the delay, increases the data delivery ratio without causing overhead, enhances the output by addressing the malevolent node attacks and which provides good power optimization, hence enhancing network lifetime.

The overview and the flow of the suggested design is represented in Figure 1. Initially, a mobile network is established to initiate communication inside the network. After the creation of MANET, cluster formation occurs by grouping of the similar nodes i.e., the nodes that shows the same characteristics and then contingent on the utility of the energy levels cluster leader is elected so that it effectively handles the transmission process. The transmission procedure is initiated with the broadcasting of the packets into the network. The packets carrying data are passed among the nodes contingent on the data present in the contiguous node.

The forwarding to the nearest node happens after getting RREP message in retaliation to RREQ message. If RREP is not receipted within a peculiar time duration, then it is assumed that node is not a part of the transmission process and hence that specific node is removed from that cluster and route error (RERR) message is received. Meanwhile, every node is frequently observed and scrutinized for any venomous activity inside the network. In constraint of malevolent activity perception, the sender is informed by sending RERR message and if no such activity is observed then RREP is delivered to the sender, which after received the message sends the data to the target. Thus, using this way effective communication occurs without any assault by the intruders.

4. Cluster Management

Clustering is a method in which the nodes that have the similar attributes are assembled together to obtain load balancing. In addition, cluster formation aids in minimizing overhead and consumption of more energy can also be reduced [9]. In this section, we discuss about the formation together with the maintenance of cluster. It could be utilized for the management of resource, location and routing management.

4.1. Cluster Formation

The motive of clustering includes the usage of network resources efficiently, enhance the accessibility

and to lessen the overheads in a network [26]. In every cluster a node features as: cluster head (CH), cluster member, gateway node and secondary cluster head. However, the foremost feature of a cluster leader is to accumulate information of the respective sensors and to carry the information to the distant processing element. To diversify the life of the battery, CH administers network management tactics to magnify network cooperation. It also lowers the extent of energy utilization by organizing activities within that cluster so that the sensor can swap to low power sleep mode. Several typical nodes are termed cluster members which has direct access to cluster head. A node which converse with two or even more cluster heads is termed as gateway node whereas the secondary cluster leader securely accumulates backup information regarding cluster and routing.

4.2. Cluster Head Selection

To appoint a cluster leader the node invokes Cluster Head module. The following steps were utilized for selecting the cluster head:

- 1 A node inside the MANET checks for smallest mobility index among non-gateway nodes.
- 2 When lowest mobility index is found, it declares itself CH and notices other nodes, otherwise it changes its status to an ordinary node.

During CH selection, every individual node telecasts its mobility details to its neighborhood nodes. Once mobility information is collected by neighbors, it starts looking for a node which has the smallest mobility index. When this node is confirmed, it turns to be CH and intimates all its neighbors.

Quality of a peculiar node is dependent on weight-based clustering [8, 21]. The CH is elected when there exists a node which has the lowest weight. The evaluation for clustering is given as:

- 1 Compute the leftover energy of a peculiar node by the formula, Remaining Energy (E) = Initial Energy - Consumed Energy.
- 2 Connectivity (C) is an estimation of the number of adjoining nodes available for the intended target nodes.
- 3 To attain mobility of any peculiar node, the formula is as follows.

$$M = \frac{1}{T} \sum_{i=1}^T \sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}.$$

4 SNR(S) of the targeted node is computed using

$$\text{SNR} = 10 \log_{10} \left(\frac{R^2}{\text{MSE}} \right).$$

Finally, the estimated parameters are combined together for weight calculation utilizing the following formula,

$$W = W_1 * E * W_2 * C * W_3 * M + W_4 * S$$

W – weight of the given node and W1, W2... are the weight factors having values among 0 and 1.

4.3. Cluster Based Detection

So far, we had a glimpse at the problems of efficient use of IDS. In our projected work, black hole strike is presented during the simulation time. Here, black hole onslaught is the dribble of information packets and in addition the forwarded messages are not broadcasted to the neighbors, such nodes are also called selfish nodes. To reduce these problems, a cluster-based routing is used.

The major problem faced by MANET is overhead caused by routing. Cluster-based routing approach provides a solution for effectively decreasing routing control overhead and improves the network scalability. To lessen the communication and control overhead, it groups similar nodes in which one node inside every cluster is elected as CH.

The major role of this design is to minimize on demand route discovery traffic and use local repair to reduce route recovery delay and to discover new route discovery.

A node forwarding HELLO MESSAGES for the adjoining nodes will have status information to it. The HELLO MESSAGE contains source address, life time and current status. The lost HELLO messages are kept in neighbor table which also contains expiration time, Neighbor ID and status.

Upon the receipt of HELLO MESSAGE transmitted from the neighbor, the node checks for its presence in the neighboring table. If a node is alive, the neighbor's expiry time is updated or else new entry is added. When a peculiar node does not receive any HELLO MESSAGES over an interval of time period it is thought to be unconnected and detached from the neighbor table.

To broadcast packets to adjoining node it sends RREQ (Route Request), if the packets are received once it sends RREP to the sender which has broadcast earlier. If the packets are not transported to the intended destination it sends RERR (Route Error).

The probability for the node monitored at security level l is:

$$P(l/k) = \sum_{i=l}^k \binom{k}{i} p^i (1-p)^{k-i}.$$

The above-mentioned formula is utilized to discover the level of certainty in a network.

Algorithm for Detection

Input: Checking black hole onslaught

Output: invoke the timer based on attack load

Step 1: Function Timer ()

Step 2: Begin

Step 3: if

{

Step 4: if (Estimated Attack Load <= Load Step)

{

Step 5: Estimated Attack Load = Load Step

Step 6: else

Step 7: Estimated Attack Load = Estimated Attack Load + Load Step;

}

Step 8: if (Estimated Attack Load > Max Allowed Load)

{

Step 9: Estimated Attack Load = Max Allowed Load

Step 10: else

Step 11: Estimated Attack Load = Estimated Attack Load;

}

Step 12: End

5. Performance Evaluation

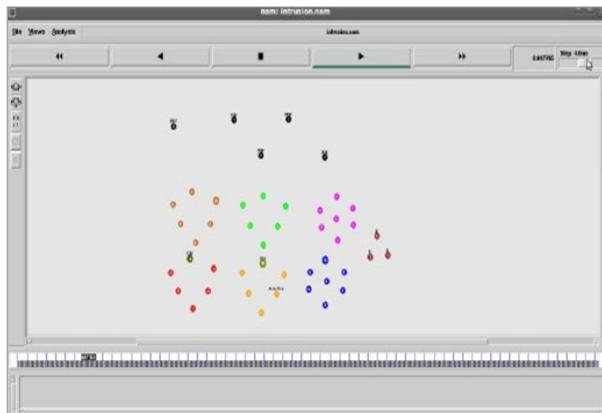
The simulation of the suggested design is realized using NS-2. The result is analyzed by varying some parameters i.e., quantity of nodes together with quantity of malevolent nodes. Here, AODV protocol is also used for routing. AODV when combined with Delay Tolerant Network minimizes the overall time con-

sumed for communication in WSN [23]. The simulation parameters are given below

Table 1
Simulation Parameters

Simulation Parameters	Values
Channel Type	Wireless
Propagation Model	Two Ray Ground
No. of Nodes	48
Data Payload	512 bytes/packet
MAC Type	802.11
Transmission Range	250
Speed	0-20m/sec
Area of Simulation	1000 x1000
Time of Simulation	120 sec

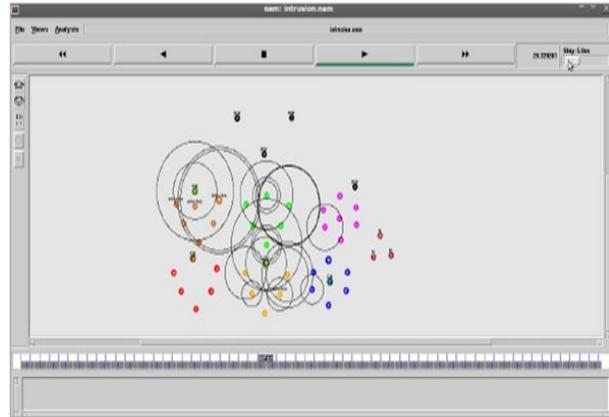
Figure 2
Detection of Intruder



A network is prone of attacks by the intruder which results in congestion and delay inside the network and hence it is more important to find the presence of invader. Using the suggested algorithm – DCAIDS, the actuality of invader can be observed. As in Figure 2, each cluster is represented in different colors and the intruder present in the cluster is shown. When invader in a cluster/path is detected, then that particular path is omitted and the sender chooses another efficient routing way for the transportation of information packets as represented in Figure 3.

The accomplishment of the suggested system is estimated for various variables like Packet Delivery Ra-

Figure 3
Changing Routing Path after Intrusion Detection

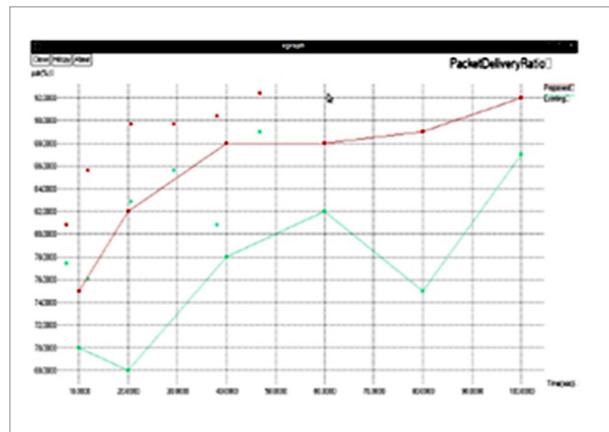


tio, End-to-end delay, Throughput and Energy Consumption. The evaluation is concluded by comparing the production of the suggested system DCAIDS and the already existing EAACK [10] for the same values.

5.1. Packet Delivery Ratio

Packet delivery proportion is nothing but the proportion of quantity of information packets transferred to the target. When reproduction time enlarges, PDR has greater value and has better performance as shown in Figure 4. This is obtained by concentrating on the sent packet, lost packet and received packet. To reduce the lost packet, data must be maintained between the nodes, thus it gives good packet delivery ratio in a network.

Figure 4
Packet Delivery Ratio



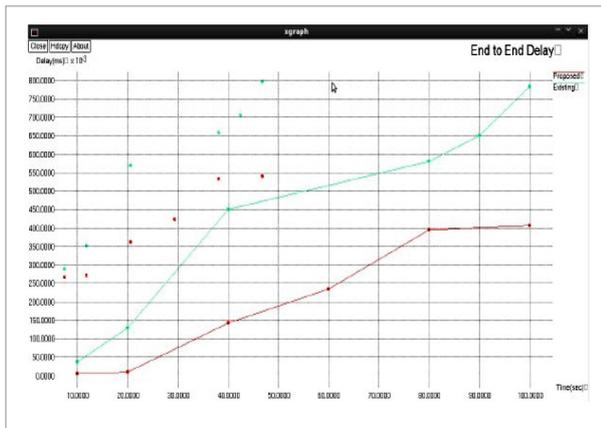
$$\text{Packet Delivery Ratio} = \frac{\text{Received Packets}}{\text{Generated Packets}} * 100$$

The proportion of packet delivery of the suggested DCAIDS is compared with the already existing EAACK, it is established that the designed system provides better delivery proportion compared to that of EAACK.

5.2. End-to-End Delay

End-to-end delay measures the aggregate time utilized by a packet carrying data to make to the target. It also considers the delay incurred by route discovery. The smaller value of delay will give better functioning in the network. Figure 5 shows end-to-end delay plot for the proposed DCAIDS with the existing EAACK.

Figure 5
End-to-End Delay



$$\text{End to End delay} = \text{Time the packet sent} - \text{Time the packet received}$$

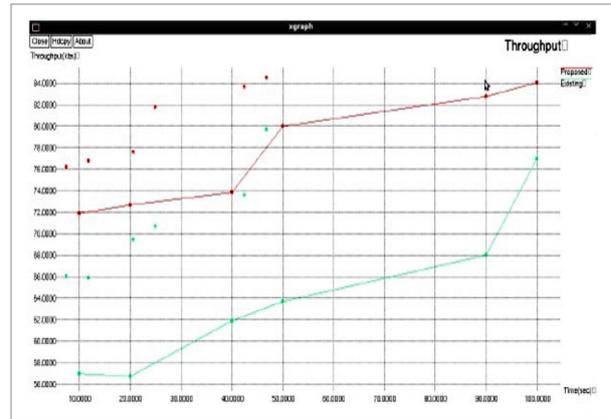
End-to-end delay for the suggested method DCAIDS is compared with EAACK, it is established that the suggested algorithm provides less delay in collation with the one which is already in existence.

5.3. Throughput

Throughput is procured by estimating the limit of supplying successful messages over a transmission network. Every packet transferred towards the destination, sometimes sent packets are not obtained at the receiver. Figure 6 represents throughput of the designed system.

$$\text{Throughput} = \frac{(\text{Number of Data packets received} * \text{Packet size} * \text{malicious node})}{\text{simulation time}}$$

Figure 6
Throughput



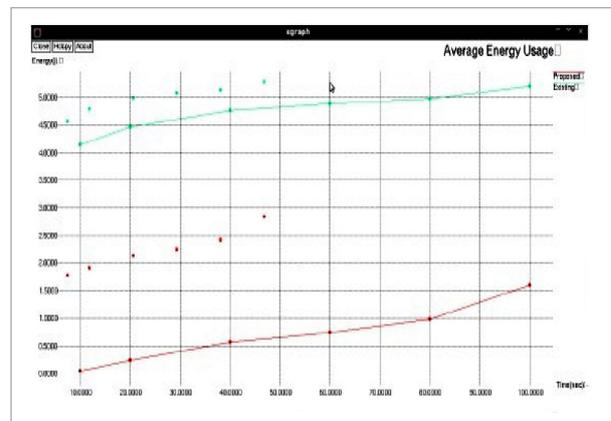
The throughput values are obtained for different time period for both DCAIDS and EAACK and its inferred that throughput of DCAIDS is better comparing to the already existing one.

5.4. Energy Consumption

Node uses its energy for every packet transmitted and every packet received. The level of energy utilized by any node during the time of simulation could be obtained by detecting distinction betwixt the present energy level and initial energy value. If there occurs an increase in time of simulation then the packet sent from sender to target will have more energy consumption. The graph represented in Figure 7 entitles moderate use of energy.

$$\text{Energy consumption} = \frac{\text{Average energy}}{\text{Total energy consumed}}$$

Figure 7
Energy Consumption



The power utilized during the transmission of information is computed and the values are observed. It is established that the power utilization of EAACK is more comparing to that of the proposed DCAIDS.

6. Conclusion

We have designed an Invader Detection System that is dependent on the distributed clustering algorithm. In this project, we have explored how to provide efficient usage of energy and also to give desired security level when the MANET is attacked by the intruder. Cluster based detection approach is developed and its idea is to elect cluster leader betwixt the nodes present in the cluster. The IDS continuously monitor every individual

node present and when the invader is detected it removes that particular node from the clustering and chooses another routing path which is short and efficient. In that way, the suggested design reduces the practicability of false data transmission thus providing reliability and security. It also minimizes the time utilized for the transportation of data thereby providing good packet delivery proportion. Since our method uses cluster-based protocol for detection it eliminates the requisite for the IDS to remain active for the whole time thus providing power optimization. Our reproduction results display that cluster formation is proficient of reducing the energy utilized on detection and also it can enlarge the output and lower the delays inside a network. Thus, network lifetime also increases significantly.

References

1. Alam, T., Aljohani, M. An Approach to Secure Communication in Mobile Ad-hoc Networks of Android Devices. *IEEE International Conference on Intelligent Informatics and Biomedical Sciences (ICI-IBMS)*, 2015, 371-375. <https://doi.org/10.1109/ICI-IBMS.2015.7439466>
2. Alam, T., Aljohani, M. Design and Implementation of an Ad Hoc Network among Android Smart Devices. *IEEE International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, 1322-1327. <https://doi.org/10.1109/ICGCIoT.2015.7380671>
3. Ali, D., Seyed, R. K., Esmail, K. Security Challenges in Mobile Ad Hoc Networks: A Survey. *International Journal of Computer Science & Engineering Survey (IJCSES)*, 2015, 6(1), 15-29. <https://doi.org/10.5121/ijcses.2015.6102>
4. Amit, S., Senthil, M. T. Routing Protocols for Wireless Sensor Networks: What the Literature Says. *Alexandria Engineering Journal, Elsevier*, 2016, 55(4), 3173-3183. <https://doi.org/10.1016/j.aej.2016.08.003>
5. Balakrishnan, K., Jing, D., Varshney, V. K. TWOACK: Preventing Selfishness in Mobile Ad-hoc Networks. *Wireless Communication and Networking Conference*, 2005, 4, 2137-2142. <https://doi.org/10.1109/WCNC.2005.1424848>
6. Basant, S., Santosh, B., Sushanta, K. Intrusion Detection in Mobile Ad-hoc Networks: Bayesian Game Formulation. *Engineering Science and Technology - an International Journal*, 2016, 19(2), 782-799. <https://doi.org/10.1016/j.jestech.2015.11.001>
7. Bhoi, S. K., Khilar, P. M. Vehicular Communication: A Survey. *IET Networks*, 2014, 3(3), 204-241. <https://doi.org/10.1049/iet-net.2013.0065>
8. Chaiang, C. C., Wu, H. K., Liu, W., Gerla, M. Routing in Clustered Multi-hop, Mobile Wireless Networks with Fading Channel. *IEEE Singapore International Conference on Networks SICON'97*, 1997, 197-211.
9. Deepti, S. Clustering Based Dynamic Load Balancing Algorithm. *International Journal of Computer Trends and Technology (IJCTT)*, 2017, 48(1), 32-35. <https://doi.org/10.14445/22312803/IJCTT-V48P108>
10. Elhadi, M., Shakshuki, N. K., Tarek, S. R. A Secure Intrusion Detection System for MANET. *IEEE Transaction on Industrial Electronics*, 2013, 60. <https://doi.org/10.1109/TIE.2012.2196010>
11. Gracy, T. W., Sakhivel, S. Fuzzy Based Intrusion Detection for Cluster-based Battlefield MANET. *IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2017.
12. Hai, H. T., Huh, E. N. Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks. *Future Generation Communication and Networking*, 2007, 1, 350-355. <https://doi.org/10.1109/FGCN.2007.175>
13. Khalil, I., Bagchi, S., Shroff, N. B. SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks. *37th Annual IEEE/IFIP International Conference on De-*

- pendable Systems and Network, 2007. <https://doi.org/10.1109/DSN.2007.88>
14. Manikopoulos, C., Ling, L. Architecture of the Mobile Ad-hoc Network Security System. IEEE International Conference on System, Man and Cybernetics, 2003, 4, 3122-3122.
 15. Marchang, N., Datta, R. Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks. Elsevier Ad hoc Networks, 2008, 6, 508-523. <https://doi.org/10.1016/j.adhoc.2007.04.003>
 16. Marchang, N., Datta, R. Lightweight Trust-Based Routing Protocol for Mobile Ad-hoc Networks. IET Information Security, 2012, 6(4), 77-83. <https://doi.org/10.1049/iet-ifs.2010.0160>
 17. Marti, S., Gjuli, T. J., La, K., Baker, M. Mitigation Routing Misbehaviour in a Mobile Ad-hoc Environment. Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000, 255-265. <https://doi.org/10.1145/345910.345955>
 18. Nadkarni, K., Mishra, A. Intrusion Detection in MANETs: The Second Wall of Defence. IEEE Industrial Electronics Society Conference, Roanoke, Virginia, USA, 2003, 1235-1239.
 19. Part, W. J., Parker, A., Joshi, M., Iorga, Karygiannis, T. Secure Routing and Intrusion Detection in Ad-hoc Networks. IEEE International Conference on Pervasive Computing and Communications, 2005.
 20. Payel, S., Asoke, N. An Overview on Mobile Ad-Hoc Networks. International Journal of Multidisciplinary Research and Modern Education, 2016, 2(1), 151-158.
 21. Prema, M., Ajay, D. A Survey of Weight-Based Clustering Algorithm in MANET. IOSR Journal of Computer Engineering, 2013, 9(6), 34-40. <https://doi.org/10.9790/0661-0963440>
 22. Rathish, C. R., Karpagavadivu, K. Cost Effective Energy Efficient Scheme for Mobile Adhoc Network. International Journal of Computing, 2020, 19(1), 137-146. DOI: 10.13140/RG.2.2.22896.61444
 23. Rathish, C. R., Prakasam, P. Hybrid Mobile Ad-Hoc Delay Tolerant Network for Optimum Routing in Wireless Sensor Networks. International Journal of Innovative Technology and Exploring Engineering, 2019, 8(11), 1303-1308. <https://doi.org/10.35940/ijitee.J9559.0981119>
 24. Rathish, C. R., Rajaram, A. Sweeping Inclusive Connectivity-based Routing in Wireless Sensor Networks. ARPN Journal of Engineering and Applied Sciences, 2018, 13(5), 1752-1760.
 25. Sheltami, T., Al-Roubaiey, A., Mahmoud, A., Shakshuki, E., Mouftah, H. AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement. 24th IEEE International Conference on Advanced Information Networking and Applications, 2010. <https://doi.org/10.1109/AINA.2010.136>
 26. Tao, W., William, N. N. H. Reliable Node Clustering for Mobile Ad Hoc Networks. Journal of Applied Mathematics, 2013, 1-8. DOI: 10.1155/2013/285967 <https://doi.org/10.1155/2013/285967>
 27. Varshney, T., Tushar, S., Pankaj, S. Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network. Communication Systems and Network Technologies, Fourth International Conference, 2014. <https://doi.org/10.1109/CSNT.2014.50>
 28. Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., Hassan, A. Vehicular Ad-hoc Networks (VANETS): Status, Results, and Challenges. Telecommunication System, 2012, 50(4), 217-241. <https://doi.org/10.1007/s11235-010-9400-5>

