Research Article

Evaluation of Trust Algorithm in a Mobile Ad-Hoc Network Using Artificial Engineering

Dr.T.Kowsalya [a], Dr.C.Selvi [b], Dr.S.Lavanya[c], Dr.J.Preetha[d], and R.Kavishree[e]

[a,b]*Department of Electronics and Communication Engineering,*
Muthayammal Engineering College(Autonomous),Rasipuram,Tamilnadu
[c,d,e] *Department of Computer Science and Engineering,*
Muthayammal Engineering College(Autonomous),Rasipuram,Tamilnadu

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: A MANET network is made up of wireless nodes which operate without a defined structure, the arrangement of existing devices does not have any ministerial or control entity . the management tasks are carried out by the teams which are in the network, therefore a MANET network is said to be a managed network. As there is no infrastructure, such as, the bandwidth, availability, input error rate, among others, depend exclusively on the behaviour of the network users. This work presents a functional solution, which decreases the energy consumption in MANET networks, implemented using game theories and genetic algorithms solution. The evaluation of the pay-as-you-go strategy from the modified prisoner dilemma was shown to be an easy to implement and interpret tool for the network equipment. The processes of generation, combination and mutation of strategies demonstrated the in-centive of cooperation in the network, observed in the increase of the average confidence of the nodes, a very high value. The intervention of the protocol with the use of genetic algorithms, demonstrated ot be a form of implementation of solutions for problems of multiple agents, the increase in the evaluation of trust of the nodes was observed, which can be interpreted as a convergence of the nodes to cooperate. The results obtained in the simulations carried out show the functioning of the algorithm implemented and the functionality of the network after its implementation.

Keywords: Wireless network, Manet, Game Theory, Trust, Accuracy, processing, Performance.

1.Introduction

A MANET network is made up of wireless nodes which operate without a defined structure, the arrangement of existing devices does not have any ministerial or control entity [1] [2], the management tasks are carried out by the teams which are in the network, therefore a MANET network is said to be a managed network. As there is no infrastructure, such as, the bandwidth, availability, input error rate, among others, depend exclusively on the behaviour of the network users [3]. In addition, transmission strategies must take into account changes in the distribution of nodes. Tasks such as: Routing, addressing, power management, among others, are of great importance since the strategies used in them would directly influence the network's desempen˜o [4]. For example, changing routes requires the transmission of configuration information, so making changes more frequently than required can decrease the efficiency of the network. However, trying to use non-existent or useless routes would also decrease the efficiency of the network since retransmissions would have to be made. Transmitting information involves energy costs, and a node is rewarded for this by the possibility of transmitting in the network. However, the team may determine not to retransmit the information, so its energy expenditure will decrease. information. This behavior is harmful to the network because of the reduction of effective nodes in the transmission [5]. Routing protocols could then help with the operation of the network if they ensure that a node that does not transmit to its neighbours (idle) has some kind of punishment and a node that cooperates with the transmission is rewarded. This will increase bateries the average battery life of the equipment and the useful time of the network, commonly called the lifetime. The implementation of this proposal was based on the application of bonding algorithms, which allow addressing problems with multiple agents and seek to reduce the required resources [6,7]. The game theory was used as a tool for the evaluation of the generated strategies and the validation was done through the NS2 network simulator software.

1.2 Trust algorithms

The operability of a network without infrastructure, evaluated by the effectiveness of communication between the nodes, depends on the behaviour of the equipment present. For this reason, it could qualify the behaviour of the network, depending on the choices of the nodes that make it up, problems such as relaying, routing, network security, depend exclusively on the behaviour of the equipment present. Different strategies have been developed to evaluate and increase the operation of the network, we find techniques that measure, evalut and make decisions based on the behavior of the devices, being the trust models one of the most implemented solutions. The general idea of the trust algorithms is to measure, evaluate and execute actions based on the definition of trust that is defined in the network. If a node has a high trust, it must have a high evaluation and it is expected that it can share the benefits of participating in the network, otherwise, the node would have penalties that can go to the separation of the network. In these solutions, measuring trust becomes a relevant task in the functioning of the network, so some strategies for the evaluation of trust in mobile Ad Hoc networks wil be presented[8]. Figure 3 shows the different strategies used in trust algorithms.

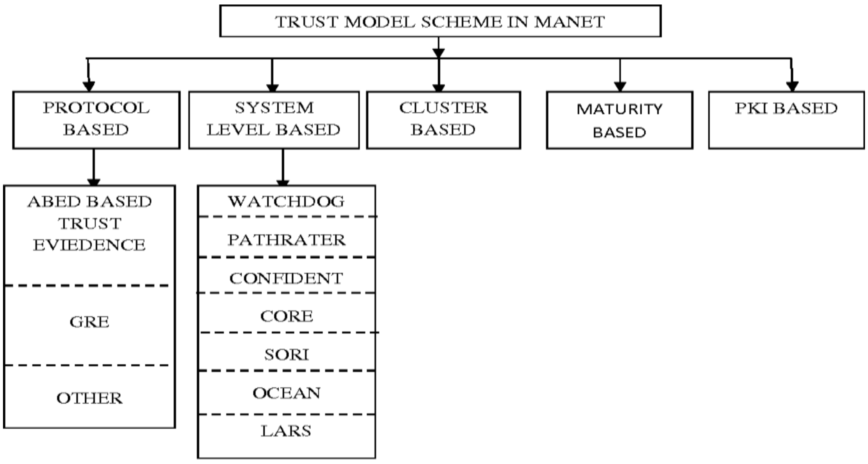


Figure 3: Types of trust strategies

1.3 Organization of paper

This paper is organized as follows. The introduction which describes the introduction of the work, the field of application and some elements to be taken into account for the construction of the project. The section address the problem, referring to the characteristics that the implemented solution must comply. In this section the main components belonging to the solution are presented, and the theoretical basis of the work carried out is present in this section of the document. In section 2 the most used routing protocols of the Ad hoc networks are presented, showing the main elements of each routing strategy and examples of some protocols. An evaluation of the existing protocols is carried out in order to determine which one would be involved and the functioning of the chosen protocol is described. In section four, the solution is described, focusing on the intervention in each algorithm and the way of construction of the main functions of the confidence algorithm, the generation and mutation of strategies and the evaluation by means of game theory In the section five the results of the intervention are presented, reviewing the operation with respect to variables such as the number of nodes.

2.Literature review

Mobile ad hoc network is wireless networking devices that customise itself and arrange itself dynamically and provide a mobile, multi-hop network. The dependency on fixed-network infrastructure is eliminated from mobile ad hoc networks by considering a mobile node as an intermediary transfer, which expands the mobile node ranges well beyond the base transceivers.The range of movable nodes is expanded beyond their level by mobile ad hoc networks[8,9]. If the nodes want to connect with other nodes outside their reach, however, the packets need to be routed from source to destination by a routing algorithms.We used AODV routing protocol because it operates in a complex network context such as MANET. What a case will lead to certain security threats. Subject to such a circumstance. Wormhole attack is one effective form of a denial of service. Because routing is the cornerstone of all mobile ad hoc communication, the whole communication will come to a standstill if routing faults occur.

[D. O. Akande and M. F. MohdSalleh, 2019] , Authors [9] offered their activities on the performance analysis of improved protocol schemes through their reconsideration, where he said that the vehicle conductive ad-hoc network on the road could be anything that any killer could enter into the network and affect the normal work of the MANET network. This requires an authentication mechanism that limits the entry of the polluted node in the MANET. This paper is a recommended advanced mid-re-encryption algorithm which reduces the overhead pattern in MANET. Through this algorithm, it reduces the proportion of the packet supply and reduces the strength of the reduction, decrease and limit the invasion in the network. The authors will be less likely to attack the MANET Convention by its new method EIRE.

[Y. Song et.al, 2019]: Authors[10] presented their paper on the survey of attacks which can be done in MANET; they presented their research on various attacks and provided comparative research on attacks and approaches to that attack surmount. The author says that in the last three or four years, the MANET attracts so much attention that due to the opportunities given to the network, many studies are around its network and to increase its ability to use it properly. Discuss about the desire for safety within the network which is required for the safety of the authors of the network. Further they provide a habitual and recycled method of surmount detailing the details of attacks on MANET and those practices. They classify these attacks in a variety of categories and provide a comparative study on this attack. The author concludes that the attack on the MANETis a serious problem because it affects the network and its functionality Make sure it is convenient but these benefits and its power cannot be used properly if these security breaches are not resolved.

[M. El-Semary and H. Diab, 2019]: Authors[11]] offered their actions on the lasting attack that it is possible to apply these attacks on MANET, even though they mention that the MANET applications are based on periodic exchange of security packets. In their coverage they say that the packets should be sent at important times, because the proper arrangements on those packets can only be reached in a timely manner. It is the responsibility of each node in the MANET network to provide the right place in the right document. When an attacker wants to attack the node network, it takes advantage of MANET vulnerabilities and attacks them. MANET attacker's protection that prevents or delay the attacker's advancement of important security messages from neighboring nodes. It can execute the replay attack by sending the facts of the event happened beforehand.
[Y. Chen, C. Hu, E. H. Wu, S. Chuang and G. Chen ,2018] [12] offered their work on a metric which is safe for delivering messages on MANET which they said that enabled wireless communication between MANET vehicles. The MANET machinery helps people with good transportation safety and efficiency. However, security issues for providing content over the infrastructure prevented wireless communication from MANET applications. They offer a civilian profit-loss Markov (APLM) model to measure the level of reliability of security systems for distribution of MANET content.The author says that the MANET belongs to the class of the genre, where mobile nodes are disconnected through wireless communication.

[Z. Chen, W. Zhou, S. Wu and L. Cheng,2020] [13]. A novel methodology based upon the study of two-hop neighbor Route Reply packet transport was proposed by fan To verify the sender 's validity, the right scheme is mandatory to produce a single key between the individual sensor node and the basis station. For their method no specific hardware or time sync is appropriate. In addition, for the proposed step of key generation only self-geographic position is needed. The mechanism of the Route Reply packet incorporates conditional transmission dependent on the legitimacy of the two-hop neighbour transmitting it. Only when each node reversed to the source node validates the two-hop sender node is the path chosen for transmission.
[Ankit Kumar et.al ,2020][14] suggested a site-based solution in which the neighbour is tested by using directional antennas. The neighbours are authenticated in the direction that the response of the HELLO message comes from and by using verifiers. The approach will detect insider attack even by authenticating the system with pair of wise hidden keys. Furthermore, this technique can only find kinds of wormholes with false neighbours.

[S. Hao, H. Zhang and M. Song, 2018] In order to avoid black hole and wormhole attack, S. Hao, H. Zhang and M. Song (2018) [15] use connexion rating schemes. They all rely on authenticated data packet identification to score links: if there is a connexion that loses packets, the recognitions will not pass; in the future the connexion is assessed as poor and prevented.
[B. Ojetunde, N. Shibata and J. Gao ,2019] suggested an approach[16] in the transmission time dependent mechanism (TTM) whereby each node noted the RREQ packet time and the RREP packet receipt time. Time consideration is also the key component in this algorithm. By excluding sender and recipient from keeping the request and reply timing, Singh et Vaisla changed this strategy.
[N. Jiang, P. Xu, Y. Yao, T. Bui and Q. Chen,2018]The findings of Mobile Ad-hoc networks (MANET) under wormhole assault have been analysed by[17]. Several QoS parameters such as the latency, latency, packet distribution ratio, energy node and node density were taken into account here.Return Routing Scheme (RRS) and Nodes Scheme Authentication (ANS). The existence of wormhole is found in this system. It operates mostly with the BSR protocol and the importance of the threshold is too important for this solution to succeed.The Stable NeighbourhooD (CECUND) protocol, which detects multi-ended gusts, was proposed by author. No need for advanced hardware, node location information or clock synchronisation specifications are positive points of this approach, but it will only operate if the presence of wormhole significantly increases fake neighbours.

[M. Ahmad, A. Hameed, A. A. Ikram and I. Wahid, 2019]The Lightweight Counter-measurement (LITEWORP) suggested[18] using guard nodes to detect the wormhole threat. After the wormhole has been found, LITEWORP leaves only the network open mode, which can cause more disruptions. To overcome this, it introduced another MOBIWORP protocol that eliminates malicious nodes from the network, locally or internationally, using central authority. They carried out work on WSN and outlined the security processes focused on the layer review of the networking protocol. The risks and vulnerabilities within them were also established. Their description of safety issues was then different. These challenges are grouped into seven categories: cryptography, key protection, attack and preventative detections; protected routing; protected location safety; and safe data fusion.They have suggested a sober approach for discovering the normal application of statistical analysis for a wormhole attack. False neighbours can detect a sensor triggered by wormhole during their proposed process of exploration, and then a k-means clustering method for detecting wormhole attacks based on their information from their neighbours.

3.Proposed Work

3.1 Trusted models

The way in which the measure of confidence is generated, allows us to divide the strategies, structures that contain the actions to be developed, into the types mentioned below we will mention the main characteristics[20] of each types:

a) **Cluster:** This trust scheme uses authentication by means of public keys in the evaluation of a node, these are grouped into clusters which allows a group of nodes to monitor the activity of the equipment directly, the nodes certify the trust of a computer which can be verified with the use of the key and a certificate issued by each neighbour, the nodes which issue trust certificates[21,22] which do not coincide with the evaluation of the Cluster would be considered "malicious" nodes and would lose the possibility of participating in the network[23,24].

b) **Social networks:** Model based on four components on each computer; Monitor that detects unusual behaviour in the nodes, reputation system that allows the nodes to be qualified acording to their routing or data transmission actions, route manager in charge of selecting the routes they present, and a trusted manager that alerts to the so-called malicious nodes. If a node shows negative behaviour that exceeds the network parameters, this will not be taken into account in the routing process, denying it the possibility of participating in the network.

c) **Non-cooperative games theory re-transmision**: Presents a model which manages trust based on the prisoner's dilemma, each node rationally making decisions about whether or not to broadcast from a neighbouring team based on a proposed strategy, which does not include the other network participants. The strategies used vary for each interaction in order to increase the payout in the game. After several executions of the game, it is expected that changes in the strategies will improve the network.

d) **Graph Model :** This model uses a graph called confidence graph, in which the vertices represent the nodes and the edges represent the confidence that the interconnected nodes have, the value of the confidence, with each interaction in the network a new edge is created or the value associated to the existing one is changed, guaranteeing the veracity of the information[25]. The nodes that have not interacted with each other must estimate the confidence measure using the measures that they have in the network, by means of averages or absolute values of the values of the network traveled.

e) **Cooperative Games Theory:** Seeks to increase the measure of trust by generating joint strategies. In this model, interactions between teams in the choice of strategies can be presented. The payment scheme of the game makes the nodes look for cooperation in the tasks of re-transmission and in the joint construction of strategies, the payment of a team will increase according to its participation in coalitions and to the extent of its collateral. The scheme seeks to increase cooperation between teams quickly and has a memory[26] limited to the behaviour exposed by the nodes in the previous iteration.**3.4 Implementation of the trust model**

After the execution of the confidence algorithm, a node decides to transmit or not. The computer uses information that comes from a neighbouring node, a hopping computer, or a distant node, however as mentioned, a node only evaluts the behaviour of its neighbours. In order to have elements of judgement about the relay of information from equipment more than one jump, a different measure of confidence must be taken into account, than information about the behaviour of distant nodes. We can evaluate the behaviour of distant nodes [27,28,29], in more than one jump, depending on the behaviour of the routes in which they participate, i.e. if a route is successful the nodes within it are "reliable". A team would then be evaluated by the behavior it presents to its neighbours and by the behavior of the routes in which it participates. In this section we will expand on the description of the confidence assessment process, both at the nodes and on the route.

3.4.1 Node confidence

The confidence you have on a node can be evaluated as the number of retransmissions it has made, having as limits the system memory, for example if the tamañ˜o of the memory is 3, a node wouldhave a confidence evaluated between zero and three. The evaluation includes indiscriminately the routing and transport packets, this value will change with each packet whose destination, at the link level, is the node to be evaluated. A node must then monitor the behaviour of its neighbouring nodes, identify the packets it is to retransmit and verify the retransmission. If the equipment retransmits, the confidence level will increase by one and if it does not detect the retransmission, the confidence level wil decrease by one[30].

3.4.2 Confidence in the Route

The teams that share information are not necessarily neighbours, so routes must be generated between source and destination teams. The correct transmission implies the cooperation of all the nodes belonging to the route. A source team will evaluate the route for the success of the transmission and a destination team will receive the information. To implement this evaluation, the fields containing the identifier of received and pending packages are used. It is not necessary to receive a confirmation of each package sent, in order to avoid errors of perception [31] . Route confidence will be evaluated as the numberof successful transmissions made, increasing if a successful transmission is detected and decreasing if a retransmission of the package is required. This evaluation would be given to the first node of the path, that is, a node would be affected by the behaviour of all the equipment it shares the path with. Finally, it should be mentioned that this measure would also be limited by a memory, the reasons for the existence of this are similar to those already expressed in the evaluation of a node, however the value of the memory of the route should be less than that of the node, since this measure depends on other equipment and as we will see later the trust in the network is greater than that related to the node.

3.4.3 Confidence-building measure in node

The confidence measure is constructed using the behaviour of a node in the face of information transmission as an input. All the nodes evalut the teams that are one jump away (neighbours) and evaluate the performance of the routes built by the AODV algorithm. The qualification obtained is of public character and is used in the evaluation of the strategy and in the decision making process of broadcasting. Each node would only be evaluated by its neighbours, since it would not be possible to have nodes in formation more than a jump away, in order to avoid the re-sending of information between nodes[32] and the consequent decrease of efficiency in the network, however, the network bond is a measure of the behaviour of nodes more than a jump away and the algorithm implemented would seek to increase this measure. The measured confidence will be the double Cn = {Cu, Cr}, where Cu represents the confidence in the node and Cr represents the confidence in the path. The possible values of Cn depend on the behaviour of node n in the last three retransmissions, a value known as the system memory, therefore Cu {0, 1, 2, 3 } this value would be equal to three if the node made the last three required retransmissions, two if it only retransmitted two of these, one if it only retransmitted one request and zero if it did not retransmit any packet. The variable Cr acts in the same way as the previous one except that it is limited to the last two transmissions and is assigned to the initial node, "first jump", of the assigned route, that is, Cr ∈ {0, 1, 2}.

Algorithm 1 : Evaluation of a node

```
function <-Confidence(neighbour)
Pass the list of neighbours()
while i! = confi.fun) do
  if i node == neighbour then
  Return confi.fun
  end if
   end while
Return 0
end function
```

Algorithms 1 shows the evaluation routine of the confidence in the retransmission of a node, for this evaluation a dynamic table is used which contains the The identification of the neighbours of a node and the evaluation of confidence in it.

3.4.4 confidence on the route

For route confidence evaluation, the transport level packets received by the final recipient are taken into account. Algorithm 2 shows the route evaluation process performed in the 802.11 protocol [33]. The memory of the route used is 2, the value returned by the evaluation in case the node is not found in the list of neighbours is 2 which corresponds to the maximum score.

Algorithm 2: Return of route evaluation

```
function CONF ROUTE(node, neighbour)
confi.fun list of neighbours()
while i! = confi.fun) do
if i.neighbour == neighbour&&i.node == neighbour then
return i. evaluate
end if
end while
Return 2
end function
```

3. Result & Analysis

Validating the behaviour of the implemented solution requires first of all verifying the behaviour of the trust measure of the devices in the network [34]. To generate this measure, the confidence that the neighbours have of a Cn node is averaged, separating the confidence by Cu retransmissions and the confidence in the Cr route.

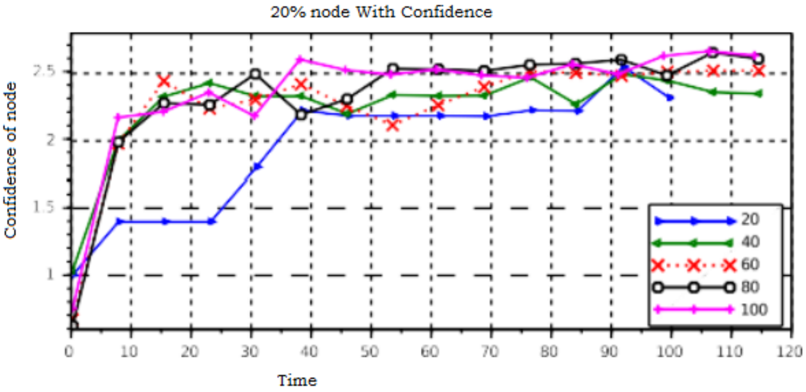


Figure 6: data transmission with Node relay confidence measure with 20%

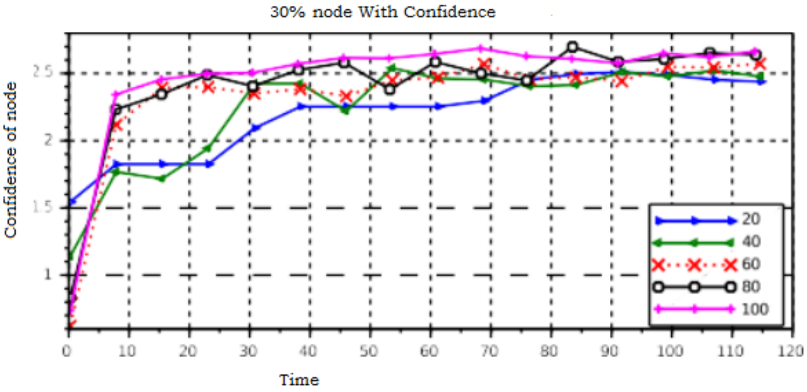


Figure 7: data transmission with Node relay confidence measure with 30%

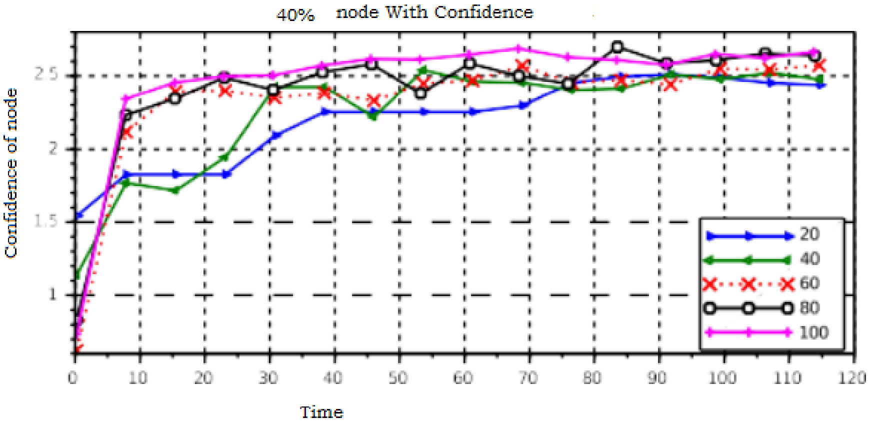
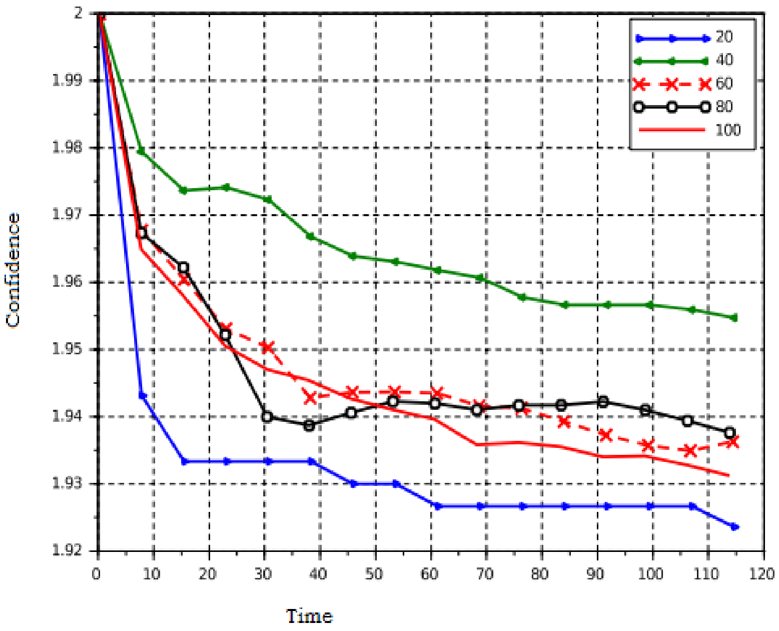


Figure 7: data transmission with Node relay confidence measure with 50%

Figure 5,6,7 shows the behaviour of the confidence measure for scenarios with different percentages of nodes acting as sources and a variable number of nodes[35]. It can be seen that the confidence measure increases over time, the final confidence values are not altered by the number of information sources, however they are affected by the number of nodes in the network, the higher confidence value is associated with scenarios containing more nodes. The solution reaches the maximum confidence value more quickly among more equipment acting as information sources. We can observe the behaviour of the confidence in the Cr network in figure 7. It is important to highlight that this measure presents a relatively low value and that the highest qualification is obtained by the scenarios with a lower number of nodes, this can be explained by the non-interference and the possible lower number of transmitting nodes.



It is then confirmed that the solution increases the confidence value of the nodes in the network, we also observe that these values tend to stabilize over time, which ensures that the solution continues to be functional for longer periods[39,40] of work.

Conclusion

This work presents a functional solution, which decreases the energy consumption in MANET networks, implemented using game theories and genetic algorithms solution. The evaluation of the pay-as-you-go strategy from the modified prisoner dilemma was shown to be an easy to implement and interpret tool for the network equipment. The processes of generation, combination and mutation of strategies demonstrated the in-centive of cooperation in the network, observed in the increase of the average confidence of the nodes, a very high value. The proposed solution showed a low dependency on the implementation scenario, factors such as the speed of the nodes, the percentage of information sources and the area of simulation did not cause changes in the informaion of the network, while factors such as the numrbeof nodes and the probability of persistence of the parent strategies significantly affected the data transmission rate.

REFERENCES

1. L. L. Njilla, H. N. Ouete and D. K. Doungwa, "Monitoring colluding behavior in MANETs using game theory," *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*, Toronto, ON, 2016, pp. 152-153. doi: 10.1109/CAMAD.2016.7790348
2. Dr.J. Preetha and Dr.S.Lavanya" Security Based Service Infrastructure for Wireless Adhoc Networks using Fuzzy Logic" PAIDEUMA JOURNAL OF RESEARCH-Web of Science, ISSN No: 0090-5674 at Volume-XIII Issue-II, FEBRUARY 2020Pg:103-108
3. J. Loganathan, Sathyaseelane, Ranjithkumar and Kirubagaran, "Enhanced load balancing scheme in MANET by using Co-Operative Game Theory approach," *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, 2015, pp. 1-5.doi: 10.1109/ICIIECS.2015.7192937
4. K. R. Reddy and A. Rajesh, "Best relay selection using co-operative game theory: MANETs," *2016 International Conference on Communication and Signal Processing (ICCSP)*, Melmaruvathur, 2016, pp. 1347-1351.doi: 10.1109/ICCSP.2016.7754372
5. S. Rai, R. Boghey and P. R. Yadav, "Cluster based energy efficient authentication scheme for secure IDS over MANET," *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*, Nagpur, 2017, pp. 200-205.doi: 10.1109/CSNT.2017.8418537
6. B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori and R. N. Mir, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks," in *IEEE Access*, vol. 8, pp. 124097-124109, 2020.doi: 10.1109/ACCESS.2020.3006043

7. A. Vij, V. Sharma and P. Nand, "Selfish Node Detection using Game Theory in MANET," *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida (UP), India, 2018, pp. 104-109.doi: 10.1109/ICACCCN.2018.8748632
8. R. Preethi and M. Sughasiny, "PBGTR: PRICE BASED GAME THEORY ROUTING FOR MINIMUM COST ROUTING PATH IN MANET," *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, Palladam, India, 2018, pp. 469-474.doi: 10.1109/I-SMAC.2018.8653603
9. Dr. J. Preetha and Dr.S.Deepajothi" Role of Sensor Network to Save Energy for Storage Nodes" Grenze International Journal of Engineering and Technology, Special Issue,ISBN:2395-5295,Vol:1,page-56-161,2019
10. Y. Song, H. Luo, S. Pi, C. Gui and B. Sun, "Graph Kernel Based Clustering Algorithm in MANETs," in *IEEE Access*, vol. 8, pp. 107650-107660, 2020. doi: 10.1109/ACCESS.2020.3001137
11. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in *IEEE Access*, vol. 7, pp. 95197-95211, 2019.doi: 10.1109/ACCESS.2019.2928804
12. Y. Chen, C. Hu, E. H. Wu, S. Chuang and G. Chen, "A Delay-Sensitive Multicast Protocol for Network Capacity Enhancement in Multirate MANETs," in *IEEE Systems Journal*, vol. 12, no. 1, pp. 926-937, March 2018.doi: 10.1109/JSYST.2017.2677952
13. Z. Chen, W. Zhou, S. Wu and L. Cheng, "An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET," in *IEEE Access*, vol. 8, pp. 44760-44773, 2020. doi: 10.1109/ACCESS.2020.2978582
14. Ankit Kumar*, PankajDadheech, Dinesh Goyal, Pawan Kumar Patidar, S. R. Dogiwal and NehaJanu, "A Novel Scheme for Prevention and Detection of Black Hole & Gray Hole Attack in VANET Network", Recent Patents on Engineering (2020) 14: 1. https://doi.org/10.2174/1872212114999200512120211
15. S. Hao, H. Zhang and M. Song, "A Stable and Energy-Efficient Routing Algorithm Based on Learning Automata Theory for MANET," in *Journal of Communications and Information Networks*, vol. 3, no. 2, pp. 43-57, June 2018. doi: 10.1007/s41650-018-0012-7
16. B. Ojetunde, N. Shibata and J. Gao, "Secure Payment System Utilizing MANET for Disaster Areas," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 12, pp. 2651-2663, Dec. 2019. doi: 10.1109/TSMC.2017.2752203
17. N. Jiang, P. Xu, Y. Yao, T. Bui and Q. Chen, "Exploiting Radio Irregularity for Location Verification in Sparse MANETs," in *IEEE Communications Letters*, vol. 22, no. 6, pp. 1284-1287, June 2018. doi: 10.1109/LCOMM.2018.2828406
18. M. Ahmad, A. Hameed, A. A. Ikram and I. Wahid, "State-of-the-Art Clustering Schemes in Mobile Ad Hoc Networks: Objectives, Challenges, and Future Directions," in *IEEE Access*, vol. 7, pp. 17067-17081, 2019. doi: 10.1109/ACCESS.2018.2885120
19. T. Rahman, I. Ullah, A. U. Rehman and R. A. Naqvi, "Notice of Violation of IEEE Publication Principles: Clustering Schemes in MANETs: Performance Evaluation, Open Challenges, and Proposed Solutions," in *IEEE Access*, vol. 8, pp. 25135-25158, 2020. doi: 10.1109/ACCESS.2020.2970481
20. Kumar A., Dadheech P., Beniwal M.K., Agarwal B., Patidar P.K. (2020) A Fuzzy Logic-Based Control System for Detection and Mitigation of Blackhole Attack in Vehicular Ad Hoc Network. In: Chaudhary A., Choudhary C., Gupta M., Lal C., Badal T. (eds) Microservices in Big Data Analytics. Springer, Singapore. https://doi.org/10.1007/978-981-15-0128-9_15
21. M. Ponguwala and S. Rao, "E2-SR: a novel energy-efficient secure routing scheme to protect MANET-IoT," in *IET Communications*, vol. 13, no. 19, pp. 3207-3216, 3 12 2019. doi: 10.1049/iet-com.2019.0039
22. S. Doss *et al*., "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," in *IEEE Access*, vol. 6, pp. 56954-56965, 2018. doi: 10.1109/ACCESS.2018.2868544
23. R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," in *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019. doi: 10.1109/TMC.2018.2828814
24. Sangeetha V. and S. S. Kumar, "ZIDS: Zonal-based Intrusion Detection System for studying the malicious node behaviour in MANET," *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, 2015, pp. 276-281.doi: 10.1109/ERECT.2015.7499026

25. J. Xie and T. Murase, "Multiple User Cooperative Mobility in Mobile Ad Hoc Networks: An Interaction Position Game," in *IEEE Access*, vol. 8, pp. 126297-126314, 2020.doi: 10.1109/ACCESS.2020.3007931
26. I. Chen, R. Mitchell and J. Cho, "On modeling of adversary behavior and defense for survivability of military MANET applications," *MILCOM 2015 - 2015 IEEE Military Communications Conference*, Tampa, FL, 2015, pp. 629-634.doi: 10.1109/MILCOM.2015.7357514
27. D. Nezník, L. Doboš and J. Papaj, "Radio Resource Management for Wireless Networks," *2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA)*, Pardubice, Czech Republic, 2019, pp. 1-6.doi: 10.1109/RADIOELEK.2019.8733591
28. R. Seetharaman, L. H. Subramaniam and S. Ramanathan, "Mobile Ad Hoc Network for Security Enhancement," *2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC)*, Chennai, India, 2019, pp. 279-282.doi: 10.1109/ICPEDC47771.2019.9036648
29. R. Chaudhry and S. Tapaswi, "Game theoretic energy aware power management in Mobile Ad hoc Networks," *2017 4th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, 2017, pp. 38-43.doi: 10.1109/SPIN.2017.8049912
30. L. Y. Njilla and N. Pissinou, "Dynamics of data delivery in mobile ad-hoc networks: A bargaining game approach," *2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Verona, NY, 2015, pp. 1-6.doi: 10.1109/CISDA.2015.7208634
31. C. Wu, M. Gerla and M. van der Schaar, "Social Norm Incentives for Network Coding in Manets," in *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1761-1774, June 2017.doi: 10.1109/TNET.2017.2656059
32. A. NAJA, M. BOULMALF and M. ESSAAIDI, "A game theoretical based rebroadcasting protocol for content dissemination in VANETs," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 591-596.doi: 10.1109/IWCMC.2019.8766594
33. B. Kasiri, I. Lambadaris, F. R. Yu and H. Tang, "Privacy-preserving distributed cooperative spectrum sensing in multi-channel cognitive radio MANETs," *2015 IEEE International Conference on Communications (ICC)*, London, 2015, pp. 7316-7321.doi: 10.1109/ICC.2015.7249495
34. L. Njilla, H. Ouete, N. Pissinou and K. Makki, "Game theoretic analysis for resource allocation in dynamic multi-hop networks with arbitration," *2017 Annual IEEE International Systems Conference (SysCon)*, Montreal, QC, 2017, pp. 1-8.doi: 10.1109/SYSCON.2017.7934772
35. J. Konorski and K. Rydzewski, "A Centralized Reputation System for MANETs Based on Observed Path Performance," *2015 8th IFIP Wireless and Mobile Networking Conference (WMNC)*, Munich, 2015, pp. 56-63.doi: 10.1109/WMNC.2015.42