International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Security Improved Chicken Swarm Optimization Based A* Routing Algorithm on MANETs

Gondi Yasoda Devi, Gurrala Venkateswara Rao

Abstract: ***The mobile devices usage has been widespread, which directly impacts the increase of mobile communication, the increased usage of Mobile Ad-hoc networks(MANETs) has brought a rapid growth in the technology development. MANETs can be deployed in any environment conveniently as it comes under the category of ad-hoc networks which is infrastructureless. Due to flexibility of deployment features, it is compatible with other networks like PAN, LAN, etc.,. MANET is applicable in many applications like rescue of emergency disasters, military operations and other special environments where wired system may not support and of urgency. Since, MANETs are having the property of infrastructureless, nature of topology of network being dynamic, and lack of authority certification leads to certain problems with regard to security from attackers. In MANETs high attention should also be given to security parameter along with other parameters for efficient routing. With the aim of facing the possibility of malicious node attacks, the proposed paper presents the technique of detecting the malicious nodes attacks caused form two major attacks like blackhole and wormhole attacks are detected and prevented by Cooperative Bait Detection Scheme (CBDS). Once those attacks are prevented, the routing efficiency in MANETs for Chicken Swam Optimization based A* algorithm is improved, which is a computer algorithm that is broadly deployed in path finding and graph traversal. The comparative examination of Optimized A*, Ad-hoc On-Demand Distance Vector (AODV) with the proposed model against attacks, enhances the performance.***

Keywords-MANETs, CBDS, blackhole, wormhole, malicious node, attack prevention

I. INTRODUCTION

MANETs are mechanized wireless communication networks that are self controlled mobile device configurations where mobile nodes cooperate with each another through wireless interfaces without hinge on any defined infrastructure [1]. MANETs are easily applicable when there is a requirement for temporary communication system without infrastructure for example: earthquake-afflicted zones and hefty wild events spot [2]. Whichever two nodes surrounded by the signal scope of the erstwhile side communicate directly; or else they can communicate all the way through other nodes. Hence, simultaneously every node mount client functions and route[3].

Manuscript published on January 30, 2020.
* Correspondence Author
Gondi Yasoda Devi*, Research Scholar, Department of CSE GIT, GITAM Deemed to be University, Visakhapatnam, mail:gondi.yasoda@gmail.com
Dr. Gurrala Venkateswara Rao, ,Department of CSE, GIT, GITAM Deemed to be University, Visakhapatnam, India. venkateswararao.gurrala@gitam.edu

Several factor of MANETs that are outstanding like dynamic network topology changes, saving of energy, node's trust. The fortification of interactions in multi-hop is dependent on the route node's consistency is the property that is verified in node's trust. Furthermore, it is noteworthy that routing protocols be acquainted with trustworthiness of nodes that are existing in the route. In addition, conventional routing protocols in MANETs visualize that the total nodes work fine, which might cause MANETs to expose against malevolent attacks. Some of the usual targets of the attack are battery power, routing protocols, and bandwidth [3].

In MANETs, the capacity of the mobile node's battery is limited, which affects the survival of the network because the links are not connected while the battery is worn out. On considering the routing protocol, the energy of the mobile nodes is necessary for ensuring the network connectivity and enhances the life span of the network [4]. These exertions craft the MANETs security to rates inferior than wired network and fabricate several security issues.

As in MANETs the open media is used to make communication, where attackers may effortlessly eavesdrop messages that are being transmitted. In MANETs considering the design of routing protocol are susceptible to many types of attacks as it is having the properties like no authority certification, with no central infrastructure, dynamic topology, transmit of data packets or route request correctly. Blackhole[5] attack is one of the frequent attack where the malicious node may exert a pull of all packets by means of sham RREP to fallaciously claim a shortest route to destination. Which is portrayed in Fig.1. Denial-of-Service attacks variant is a black-hole attack, grayhole attack is another variant of blackhole attack which selectively castoffs and aheads data packets in the process of packet transmission. In Cooperative blackhole attack many malevolent nodes cooperate with apiece and grouply work. To all the networks massive harm is caused by these kinds of attacks which resulted in many detective methods to fail.

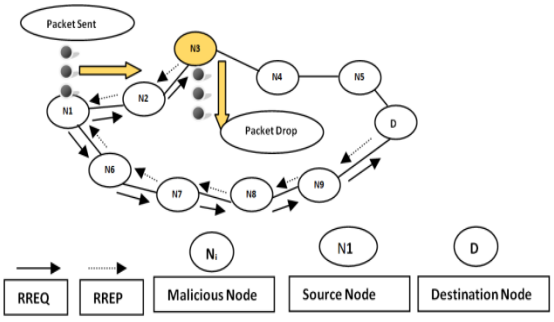


Fig.1 Blackhole attack–Packets dropped at node N_3

The adjacent node's address is used as destination bait address, which baits malevolent nodes for RREP reply and the program which reverse traces the path and malevolent nodes are detected. Ultimately the malicious nodes that are detected are listed in a blackhole list and make a notice to other nodes of the network to not to communicate with those malevolent nodes. Coming to the result, the proposed algorithm is able to reduce the drop of packets and which inturn increases the delivery ratio of packet. The major contributions of the paper are depicted as follows

- To model the MANET routing protocol with attack detection and prevention model using CBDS, especially focussing blackhole and wormhole attacks in an optimized A* algorithm using improved CSO algorithm termed as FPR-CSO for accomplishing the obstacle-aware MANET routing, in which the CE-OLSR performs the obstacle detection.
- To performs the FPR-CSO- A*-based MANET routing by concerning the constraints like node availability, distance of the path, and congestion of each node.

II. LITERATURE REVIEW

A. Related Works

Different researches suggested diverse solutions in detecting the malevolent nodes. But, in these conventional solution only the single malevolent node can be detected or much resource and time is to be costed for cooperative blackhole detection.

There are some researchers propose diverse solutions about detecting malicious node. However, most these methods just can detect single malicious node or need to cost much time and resource to detect cooperative black hole. Even these methods require specific environment to perform and need many premises and assumptions.

Constant monitoring of the nearest nodes is followed in proactive[6][7] algorithms. The resources here are wasted for constantly being on the task of finding the malicious nodes despite of existence or not. But coming to it's advantage of avoiding the possibility of attack at the initial juncture of MANETs but due to it's constant monitoring drops the performance. When there is significant packet drop the reactive routing algorithms[8] [9] will trigger in the process of packet transmission. These type of approaches in MANETs are still suffering from packet drops at any stage in the network which is harming the final result in the wireless networking system.

In 2019, Muneeswari et al.,[10] has recommended an ESCT model, which resembles human cognitive procedure and depend on trust-level data for avoiding different routing disruption attacks. Moreover, mobile nodes interchanged the confidential data and evaluate received confidential data on the basis of cognitive opinion. Finally, every node vigorously progress its cognition for eliminating malicious entities. The more interesting characteristic of ESCT was that it won't cooperate the model still the internal hackers have an idea of the working of security system. The efficiency of the ESCT system was analysed by various routing disruption attack conditions. At last, the experimental outcomes have confirmed that the ESCT model has promoted network scalability and assured the routing efficiency.

In 2016, Malathi et al[11] had introduced MBRA approach for decreasing the ACK overhead and eradicating the malicious attacks. The BAP was grasped by suggested approach using cluster heads, which utilized optimal bandwidth for sending the data packets by routing the nodes in clockwise and anti-clockwise routing procedure that identified and conquered the malicious attacks with an IDS/IPS coupled methodology. Moreover, the IDS approach uses the cluster heads, which were utilized for obtaining the ACK from the cluster nodes at the time of packets transfer from it. The developed approach has overcome the before specified issues and along with that its bandwidth usage was improved, and the increased the delivery of packet with low delay when contrasted over conventional approaches.

In 2011, Jian-Ming Chang et al.,[12] proposed CBDS algorithm a detection scheme for malevolent node and the induction of cooperative blackhole, grayhole or blackhole attackers. The architecture poposed is defensive architecture which integrates the reactive and proactive systems. By making use of adjacent node's address as the destination bait, the source point cooperates randomly with those nodes, the malicious nodes are made to send reply RREP message by bait system. The proposed program does reverse tracing where the malicious nodes are detected and prevented from attackers.

Marti et al. [6] dicussed a black hole detection technique where it consists of path-rater and watchdog. The malicious node is detected by overhearing the neighbour nodes by watchdog. While transmission path router assign some default value firstly and after that for each node, transmitted behaviour is being kept in observation. Based on transmitted behaviour the value changes. If observed later on with time based, the value lies underneath the threshold, the node is added to the list of blackhole

Vishnu K et al. [7] recommended the technique where Backbone nodes as a cluster of nodes that are powerful taking into consideration of range and battery. For newly incoming nodes are being allocated the Restricted IP address(RIP) this leads to the formation of Backbone network (BBN). The unused RIP id requested by BBN to send data when ever the source nodes(SN) desire to broadcast data. In this process the SN broadcast RREQ to RIP and destination simultaneously. In case the SN receives only the RREP by destination, this proves that the network is sage with not attacks, else if the SN receives from RIP the RREP – there is black hole attack in that route. The next step initiated by SN after finding the attack is to send a monitoring message for alerting the neighbour nodes to move to mode of promiscuous and make them initiate to listen to the network. To the destination some data packets that are dummy are being broadcasted by the SN. Before forwarding the packets to it's neighbour the other nodes can also observe the situation. The SN will getting the situation information from monitoring nodes, if it is observed by those nodes that packet loss is ahead the usual case. However, MANETs design there is no such network as Backbone, to say fact this system is applicable to only some system. Cooperative blackhole attacks may not be handled by theses methods. Since, neighbouring nodes collude with one another, which may result in misjudgement. These attack degrades the performance level by dropping the packets in transmission.

III. COOPERATIVE BAIT DETECTION SCHEME

The proposed paper depicts the detection and prevention scheme of malicious node. The CBDS is the scheme which launches the black and warm hole attack detection and prevention. This system works both for reactive and proactive integrated and individual defence architectures where source node cooperates randomly with adjacent stochastic nodes. The malicious nodes attacks are prevented by means of considering the address of the flanking nodes as bait target address, to get reply RREP it baits malevolent nodes and the proposed program traces and prevents the malevolent node's attacks. Whenever there is significant packet drop and decrease in the ratio of packet delivery, it is assumed that an alarm by destination node has to be sent to source node to identify and iterate the detection mechanism, to increase the maintenance capabilities and ensures the reactive response immediately. By implementing this mechanism in the proposed improved FPR-CSO based A* routing algorithm for finding the routing against obstacles and also attacks form malevolent nodes. In this process of malevolent nodes detection this scheme creates and make use of the baiting $RREQ'$ packets.

IV. PROPOSED SYSTEM

Proposed Flow for Attack and Obstacle Aware Routing in MANET

In the past years, many researchers had dedicated their precious time for improving the efficiency of MANETs routing algorithms. The main intend of this paper is to develop obstacle-aware routing protocol in MANET using optimized A* algorithm. The proposed model also focuses on detecting and preventing the major attacks like blackhole and wormhole attacks. The flow diagram of the proposed MANET routing is shown in Fig. 2

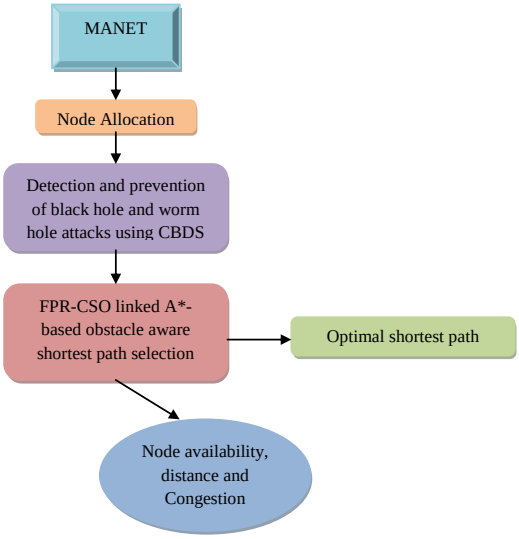


Fig.2. Diagrammatic representation of proposed Secure MANET Routing

Initially, the number of nodes in the MANET should be allocated at specified places. Since the MANET make use of open air medium for communication, they happen to suffer from high sensitive security issues when compared over the wired medium. Blackhole and wormhole attacks are considered as two such critical issues. A malicious node utilizes its own routing direction in order to make known the other nodes that it is route's shortest path to reach destination, and it doesn't forward the packets to the consequent nodes that are authorized, instead it drops the packets which is categorized as blackhole attack. On the other hand, a malicious node utilizes the artificial link to communicate the data from one end to other end of the network; by showing trust to the distant network nodes is termed as wormhole attack. These two types are attack are planned to detect and prevent by the CBDS approach. Once the attack nodes are removed from the network, the obstacle aware shortest path selection is performed by the algorithm

V. ATTACK PREVENTION AND OBSTACLE AWARE ROUTING PATTERN IN MANET USING A* ALGORITHM

A. Detection and Prevention of Attacks

Before taking an optimal shortest path concerning the obstacles, two main attacks, such as wormhole and blackhole attacks have to be recognized and prevented. In fact, "a black hole attack [13] is cited as dropping of packets from that node and sends counterfeit routing packets to route packets by and of itself". The malicious node in the network tries to take all information of the transmitted packet, which in turn leads to drop the entire packets being transmitted. On the other hand, in wormhole attack [14], "two distant malevolent nodes can be in cahoots with using either directional antenna or wired link, to give an intuition that they are only one hop away". This type of node is mostly in hidden state. The traffic of the network can easily be analyzed by the wormholes.

Operation of CBDS to detect and prevent blackhole attack: For identifying the blackhole attack, the bait process [13] tries to send a reply $RREP$ for the request $RREQ'$ from the source node. Let ne_s be the source node, and ne_d be the destination node. The adjacent node selected by the source node is represented as ne_A to which the data is to be transmitted. At first, a request message $RREQ'$ is transmitted from the source node, which involves the information like source ID IDn_s, destination ID IDn_d, and path length as given in Eq. (1). The total number of hops to forward the request message from source node to destination node is named as path length PL.

$$RREQ' = \{IDne_s, IDne_d, PL\} \quad (1)$$

The other nodes in the network send the feedback for the request message in the form of reply $RREP$ represented in Eq. (2), which indicates that the request effectively reached the final node.

$$RREP = \{IDne_s, IDne_d, PL\} \quad (2)$$

After receiving the feedback packet $RREP$ by the source node, it compares with $RREQ'$. The path length $PL = 0$ indicates that the corresponding node is the destination node. As the information regarding the destination node and path length is already stored in $RREQ'$, it can find the malicious node easily. The exact destination node is confirmed, if IDn_d in $RREQ'$ is equal to IDn_d, and $pl = 0$. If the malicious node is detected, the network discards it, and selects an alternate path for communication.

CBDS Algorithm:

1. $IDne_s$ randomly selects cooperative bait address of one hop $IDne_A$, to bait malevolent node
2. Dispatch bait RREQ' which includes $\{IDne_s, IDne_d, PL\}$.
3. If any node reply RREP which includes $\{IDne_s, IDne_d, PL\}$ from other rout except n_r
   i. If IDn_d in $RREQ'$ is equal to IDn_d in RREP and $pl = 0$

      No malicious nodes is detected

      else

      Malicious node is detected

4. Source node send RREQ
5. If respond RREP is from exact destination address

   System is normal and instigate to transmit data packets

   If there is threshold drop packet delivery ratio
   goto step 2
   else
   goto 7

   else

   goto 4

6. If exceed discovery hop limit
   goto 7

   else goto 4

7. Stop

B. Performance Analysis without Attack Detection

The performance analysis of the developed FPR-CSO – based A* algorithm over the conventional algorithms for MANET routing is tabulated in Table II for nodes 78. From Table II, the throughput of the proposed FPR-CSO-A* is 63.4% better than A*, and 50.8% better than AODV. Moreover, the cost function of the developed FPR-CSO is 18.4% improved than A*, and 78.3% improved than AODV. Moreover, when considering the number of nodes as 108, the performance of the proposed and the existing models are given in Table III, where the cost function of the suggested FPR-CSO-A* is 65% enhanced than AODV, 15.1% enhanced than A*, 1.1% enhanced than CSO. Therefore, the above results have shown that the proposed model is outperforming in determining the optimal shortest path. In Table IV, the performance of the suggested model is described and the nodes considered here are 128. In addition, the throughput of the improved FPR-CSO-A* is 48.1% superior to AODV, 83.9% superior to A*, 25.9% superior to CSO. Similarly, the total cost function of the proposed FPR-CSO is 4.8% improved than AODV, 2.4% improved than A* and 53% improved than CSO. Table V describes the performance of the modified and the traditional algorithms when the number of nodes is considered as 158. Thus, the total cost function of the proposed FPR-CSO-A* is 46.1% better than AODV, 7.7% better than A*, and 4.6% better than CSO. Thus, from the above results, it has been proven that the proposed algorithm is superior to the conventional algorithms in determining the optimal shortest path.

TABLE I. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 78 NODES WITHOUT ATTACK DETECTION

Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	176.29	67.52	68.063	68.063
Congestion Cost	15.882	25.638	8.1075	8.1075
Penalty for Node Availability	160	0	0	0
Delay	0.71	0.35	0.38	0.38
Packet Loss	0.1	0.34	0.02	0.02
Throughput	126.76	94.286	257.89	257.89
Total Cost	352.99	93.859	76.575	76.575

TABLE II. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 108 NODES WITHOUT ATTACK DETECTION

Measures	AODV	A*	CSO-A*	FPR-CSO-A*
Path Length	194.29	130.03	145.73	145.25
Congestion Cost	2.1272	40.416	1.2343	0
Penalty for Node Availability	220	0	0	0
Delay	0.71	0.68	0.57	0.56
Packet Loss	0.08	0.69	0.02	0.03
Throughput	129.58	22.794	171.93	173.21
Total Cost	417.22	171.86	147.57	145.85

TABLE III. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 128 NODES WITHOUT ATTACK DETECTION

Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	217.36	186.39	206.61	202.01
Congestion Cost	9.269	44.007	13.445	7.367
Penalty for Node Availability	220	0	0	0
Delay	0.71	0.61	0.63	0.5
Packet Loss	0.07	0.62	0.03	0.03
Throughput	130.99	31.148	153.97	194
Total Cost	447.41	231.66	220.72	209.91

TABLE IV. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 158 NODES WITHOUT ATTACK DETECTION

Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	247.45	217.22	233.38	227.59
Congestion Cost	16.943	37.1	13.642	7.8996
Penalty for Node Availability	170	0	0	0
Delay	0.65	0.74	0.58	0.56
Packet Loss	0.06	0.75	0.04	0.03
Throughput	144.62	16.892	165.52	173.21
Total Cost	435.11	255.87	247.65	236.09

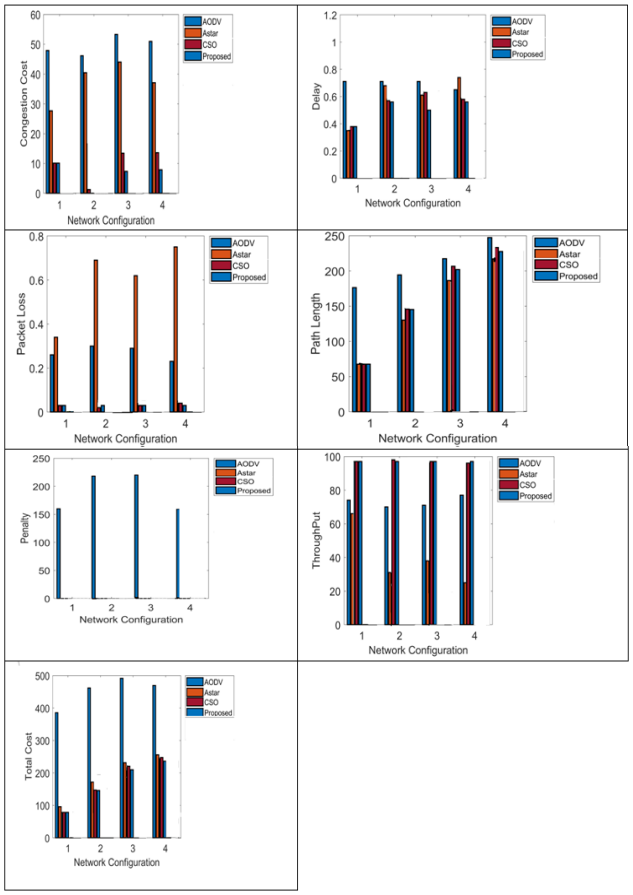


Fig.3. Graphs represtinting Performance analysis without attack detection

C. Result Analysis with Attack Detection

The performance analysis of the proposed and the existing models with attack detection are given in Table V, Table VI, Table VII, and Table VIII for different number of nodes, respectively. From Table V, the cost function of the developed FPR-CSO-A* is 78.3% superior to AODV, 18.4% superior to A*. Finally, it is shown that the proposed algorithm is well defined in determining the optimal shortest path. In Table VI, the nodes considered are 108, and the throughput of the developed FPR-CSO-A* is 29.3%, 86.4% and 7.1% better than AODV, A* and CSO, respectively. Therefore, it is confirmed that the suggested model is superior in finding the optimal shortest path. From Table VII, the performance analysis of the suggested and the existing algorithms are determined. Here, the number of nodes considered is 128. The cost function of the recommended FPR-CSO-A* is 53% improved than AODV, 9.3% improved than A* and 4.9% improved than CSO. In Table VIII, the performance of the suggested model is described, and the nodes considered here are 158. Moreover, the throughput of the modified FPR-CSO-A* is 17.2% superior to AODV, 89.6% superior to A* and 4.6% superior to CSO. Hence, it has been confirmed that the suggested algorithm is performing well in finding the shortest path after the attack prevention.

TABLE V. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 78 NODES WITH ATTACK DETECTION

Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	176.29	67.52	68.063	68.063
Congestion Cost	15.882	25.638	8.1075	8.1075
Penalty for Node Availability	160	0	0	0
Delay	0.71	0.35	0.38	0.38
Packet Loss	0.04	0.34	0.02	0.02
Throughput	135.21	94.286	257.89	257.89
Total Cost	352.93	93.859	76.575	76.575

TABLE VI. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 108 NODES WITH ATTACK DETECTION

Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	194.29	130.03	145.73	145.25
Congestion Cost	2.1272	40.416	1.2343	0
Penalty for Node Availability	220	0	0	0
Delay	0.71	0.68	0.57	0.56
Packet Loss	0.02	0.67	0.01	0
Throughput	138.03	24.265	173.68	178.57
Total Cost	417.15	171.84	147.56	145.82

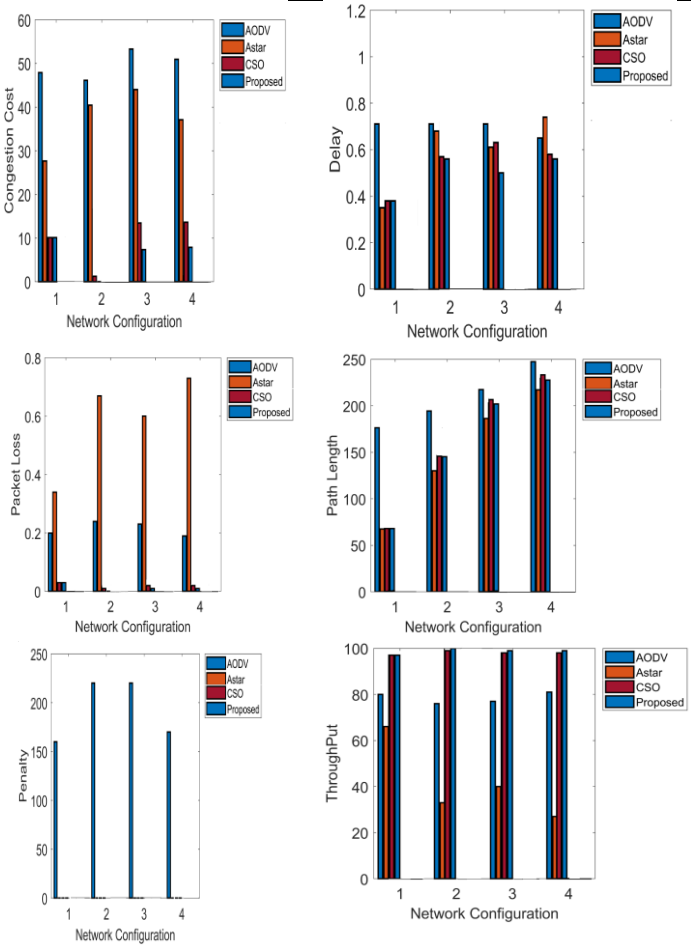
TABLE VII. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 128 NODES WITH ATTACK DETECTION

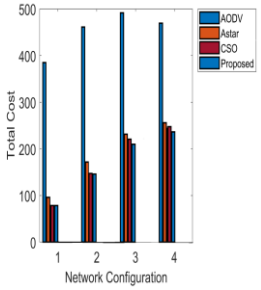
Measures	AODV	A*	CSO	FPR-CSO-A*
Path Length	217.36	186.39	206.61	202.01
Congestion Cost	9.269	44.007	13.445	7.367

Penalty for Node Availability	220	0	0	0
Delay	0.71	0.61	0.63	0.5
Packet Loss	0.01	0.6	0.02	0.01
Throughput	139.44	32.787	155.56	198
Total Cost	447.35	231.64	220.71	209.89

TABLE VIII. PERFORMANCE ANALYSIS OF PROPOSED AND CONVENTIONAL OBSTACLE-AWARE MANET ROUTING FOR 158 NODES WITH ATTACK DETECTION

Measures	**AODV [34]**	**A* [29]**	**CSO-A* [26]**	**FPR-CSO-A***
Path Length	217.36	186.39	206.61	202.01
Congestion Cost	9.269	44.007	13.445	7.367
Penalty for Node Availability	220	0	0	0
Delay	0.71	0.61	0.63	0.5
Packet Loss	0.02	0.73	0.02	0.01
Throughput	150.77	18.243	168.97	176.79
Total Cost	435.07	255.85	247.63	236.07





VI. CONCLUSION

This paper has proposed an approach by implementing a MANET routing with the help of secured FPR-CSO based A* algorithm. The routing issue of security from attackers in MANET was resolved using CBDS over FPR-CSO based A* algorithm, which was utilized for determining the path and graph traversal. Moreover, the algorithm effectively finds the malicious nodes, prevents them and plotted a walk able path among several nodes on the graph; as a result it provided a shortest path without any obstacles and free of attackers. In order to enhance the A* algorithm, the improved meta-heuristic algorithm named secured FPR-CSO was utilized. Matlab simulator is used to simulate the proposed solution and comparison is made by considering the properties like overheads and ratio of packet delivery. Finally it is observed after execution of CBD based FPR-CSO-A* in the simulator that the proposed algorithm yields an improvement in performance level with regard to ratio of packet delivery which in turn reduces the overhead in the network due to malevolent node's attacks. From the experimental results, the total cost function of the proposed secured FPR-CSO-A* was 4.8% improved than AODV, 2.4% improved than A*, 53% improved than CSO. Thus, all the protocols meanwhile show different performance with improvement in proposed model.

REFERENCES

1. Wei Quan, et al., "Content retrieval model for information-center MANETs: 2-dimensional case," 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, 2013, pp. 4422-4427.
2. Kohei Arai, et al., "Decision Making and Emergency Communication System in Rescue Simulation for People with Disabilities", International Journal of Advanced Research in Artificial Intelligence, vol.2, no.3, March 2013.
3. WolfgangKiess, et al., "A survey on real-world implementations of mobile ad-hoc networks", Ad Hoc Networks, vol.5, no.3, pp.324-339, April 2007.
4. Jieying Zhou, et al., "Ad Hoc On-Demand Multipath Distance Vector Routing Protocol Based on Node State", Communications and Network, no.05, vol.03, pp.408-413, January 2013.
5. A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journal of Computer Science and Information Security," Vol. 7, No. 1, 2010.
6. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.
7. V. K and A. J PAUL, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks," 2010 International Journal of Computer Applications, Vol. 1, No.22, 2010

8. W. Kozma, and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009.
9. W. Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," 28th International Symposium on Reliable Distributed Systems September 2009
10. R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," IEEE Transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019.
11. M. Malathi, and S. Jayashri, "Modified Bi-directional Routing with Best Afford Path (MBRBAP) for Routing Optimization in MANET", Wireless Personal Communications, vol.90, no.2, pp 861–873, September 2016.
12. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" 1932-8184 © 2014 IEEE
13. Chang, P. Tsou, I. Woungang, H. Chao and C. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.
14. MuhammadImran, Farrukh AslamKhan, TauseefJamal, and Muhammad HanifDurad, "Analysis of Detection Features for Wormhole Attacks in MANETs", Procedia Computer Science, vol.56, pp.384-390, 2015.
15. I. Kacem, B. Sait, S. Mekhilef and N. Sabeur, "A New Routing Approach for Mobile Ad Hoc Systems Based on Fuzzy Petri Nets and Ant System," IEEE Access, vol. 6, pp. 65705-65720, 2018.
16. Z. Wang, Y. Chen and C. Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 859-868, Feb. 2014.
17. WolfgangKiess, and MartinMauve, "A survey on real-world implementations of mobile ad-hoc networks", Ad Hoc Networks, vol.5, no.3, pp.324-339, April 2007.
18. Wei Quan, Jianfeng Guan, Changqiao Xu, Shijie Jia, Junlong Zhu and Hongke Zhang, "Content retrieval model for information-center MANETs: 2-dimensional case," 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, 2013, pp. 4422-4427.
19. M. R. Pearlman and Z. J. Haas, "Determining the optimal configuration for the zone routing protocol," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1395-1414, Aug. 1999.
20. G. Zhan, W. Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, March-April 2012.
21. F. Bao, I. Chen, M. Chang and J. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.
22. A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," IEEE Access, vol. 7, pp. 95197-95211, 2019.
23. Abdelfettah Belghith, Mohamed Belhassen, Amine Dhraief, Nour Elhouda Dougui, and Hassan Mathkour, "Autonomic Obstacle Detection and Avoidance in MANETs Driven by Cartography Enhanced OLSR", Mobile Information Systems, Volume 2015.
24. SeyedaliMirjalili, Seyed MohammadMirjalili, and AndrewLewis, "Grey Wolf Optimizer", Advances in Engineering Software, vol.69, pp.46-61, March 2014.
25. SeyedaliMirjalili, and AndrewLewis, "The Whale Optimization Algorithm", Advances in Engineering Software, vol.95, pp.51-67, May 2016.

AUTHORS PROFILE

Mrs. G. Yasoda Devi, (Ph.D), research scholar, department of Computer Science and Engineering, GIT, GITAM Deemed to be university, Visakhapatnam. Working as assistant professor in the Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Jonnada, Vijayanagaram. My interested areas of research are Networks, MANETs, Machine Learning.

Dr. Gurrala Venkateswara Rao, Professor, Department of CSE, GIT, GITAM Deemed to be university, Visakhapatnam, Andhra Pradesh. Research areas of interest include Networks, Mobile Computing and Software Engineering. Around 50 papers have been published in various conferences and journals. Five Ph.D's have been awarded under his guidance. He also completed a major UGC project.