Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.026137
Article

Tech Science Press

An Improved Multi-Objective Particle Swarm Optimization Routing on MANET

G. Rajeshkumar[1,*], M. Vinoth Kumar[2], K. Sailaja Kumar[3], Surbhi Bhatia[4], Arwa Mashat[5] and Pankaj Dadheech[6]

[1]Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, 638057, Tamil Nadu, India
[2]Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, 560082, India
[3]Department of Master of Computer Applications, M. S. Ramaiah Institute of Technology, Bangalore, 560054, India
[4]Department of Information Systems, College of Computer Science and Information Technology, King Faisal University, Riyadh, 11533, Saudi Arabia
[5]Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, 21911, Saudi Arabia
[6]Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, 302017, Rajasthan, India
*Corresponding Author: G. Rajeshkumar. Email: rajeshkumargrkphd@gmail.com

Received: 16 December 2021; Accepted: 09 February 2022

Abstract: A Mobile Ad hoc Network (MANET) is a group of low-power consumption of wireless mobile nodes that configure a wireless network without the assistance of any existing infrastructure/centralized organization. The primary aim of MANETs is to extend flexibility into the self-directed, mobile, and wireless domain, in which a cluster of autonomous nodes forms a MANET routing system. An Intrusion Detection System (IDS) is a tool that examines a network for malicious behavior/policy violations. A network monitoring system is often used to report/gather any suspicious attacks/violations. An IDS is a software program or hardware system that monitors network/security traffic for malicious attacks, sending out alerts whenever it detects malicious nodes. The impact of Dynamic Source Routing (DSR) in MANETs challenging blackhole attack is investigated in this research article. The Cluster Trust Adaptive Acknowledgement (CTAA) method is used to identify unauthorised and malfunctioning nodes in a MANET environment. MANET system is active and provides successful delivery of a data packet, which implements Kalman Filters (KF) to anticipate node trustworthiness. Furthermore, KF is used to eliminate synchronisation errors that arise during the sending and receiving data. In order to provide an energy-efficient solution and to minimize network traffic, route optimization in MANET by using Multi-Objective Particle Swarm Optimization (MOPSO) technique to determine the optimal number of clustered MANET along with energy dissipation in nodes. According to the research findings, the proposed CTAA-MPSO achieves a Packet Delivery Ratio (PDR) of 3.3%. In MANET, the PDR of CTAA-MPSO improves CTAA-PSO by 3.5% at 30% malware.

Keywords: MANET; intrusion detection system; cluster; kalman filter; dynamic source routing; multi-objective particle swarm optimization; packet delivery ratio

1 Introduction

Instead of using physical network connections, wireless network protocols use a type of radio signal in the air to send and receive signals [1]. The best thing about these wireless networks is that they eliminate the need for expensive network cable installation and accompanying maintenance costs. Wireless technology has a number of benefits in computing, including faster response to comments, minimal time is spent on documentation, more time spent for online users, *Just-In-Time* (JIT) and real-time control, and closer connectivity between client and host node. For many purposes, including environmental control, military operations, and recovery data plans, an ad-hoc network is used. With minimal computer and detecting equipment, the nodes in MANET must maintain exact time synchronization when gathering and disseminating data from wireless nodes. For dispersed data collection and supervision, a reliable transmission rate is essential [2].

MANET is a system of mobile nodes which lacks a wired connection, allowing nodes in the network to act as routers. Mobile nodes traverse the network and interact with one another; there are still no fixed Base Stations (BS). Routing algorithm principles that regulates the routing path reserved by message packets in networks from sender to receiver nodes. Because MANET must be smaller and has limited capacity, the primary concern in wireless devices are PDR optimization, network setup size and configuration cost reduction, low-power network, user security, and Quality of Service (QoS) [3].

Due to mobile nodes, risks from hacked nodes within the network, minimal physical privacy, dynamic topology, flexibility, and lack of centralized administration, MANETs are much more vulnerable than wired networks. MANET is more vulnerable to malicious attacks as an outcome of these flaws. Because of its insufficient physical security, new adoptions of network structure minimised energy-constrained activities, and lack of central administration, a MANET is far prone to damage than a wired network. Authenticity, data integrity, secure communication, and confidentiality are all essential security features for a successful MANET [4]. This research study investigates several forms of network threats to MANETs, and a few routing solutions. The number of average linked routing paths is affected by the mobility of the nodes, which in turn influences the routing algorithm's effectiveness. Routing in MANET is the method of determining the optimised routing path for network traffic among other networks.

This article presents a new trust-based TWOACK (2-ACK) technique for wireless networks that is effective for MANET, despite the fact that their goals are distinct. First, present a unique CTAA to protect MANET, expand the study of MANET by improving Energy-Aware Trust-based IDS with AACK for MANET, and finally, investigate wireless network route optimization employing Multi-Objective Particle Swarm Optimization (MOPSO) and its effect on MANET [5]. We suggested a consensus-based Median Kalman-Filtering Time Synchronization Method (MK-FTSS) for MANETs in this research investigation, which minimises synchronisation convergence time by efficiently disseminating the time data retrieved from the median values of synchronisation messages over an entire MANET. Furthermore, the suggested technique employs a Kalman-Filter (KF) in the synchronized information processing to eliminate synchronisation errors [6].

2 Related Works

MANET routing is categorized into reactive and proactive routing, and these are further subdivided into hybrid routing, hierarchical techniques, geographical systems, multi-path, multicast, and Geocast routing. When connecting a MANET to the online, the most often implemented routing methods are reactive and proactive, known as AODV and DSDV [7]. The Integrated Cross Interior approach is used in the IDS routing, and it was created and tested in the MANET to determine routing costs and response time. The Integrated Cross Interior method is an essential technique used for packet distribution and data protection with secure IDS transmission. The Integrated Cross Interior method was developed, and it was combined with the Nearby Path Secure Routing Algorithm based on Past Interaction History. Various metrics such as Attacker Detection Ratio, Cluster Distance (CE Distance), Overhead and Throughput measure were also evaluated and compared [8].

The goal of multipath routing algorithms is to discover new strategies for power-efficient route construction and reliable data packet relaying between source-destination pairs to maximise network lifetime. Many power-efficient routing strategies have been developed to manage specific constraints in MANETs. Many researchers have demonstrated MANET cross-layer optimization strategies that are both energy and cost-effective [9]. Some of these researches have looked into the impact of energy efficiency and other performance evaluation methods, including scalability, integrity, and EED in the existence of data transfer of energy in the network. Furthermore, in some cross-layer research, the Physical (PHY), Medium Access Control, and routing protocols are rebuilt using a Cross-Layer Design (CLD) to maximise the rate at which energy is utilised instead of lowering overall data energy consumption [10].

The computational intelligence approach are increasingly used in a wide range of real-time applications [11]. To overcome network challenges, some studies have used Genetic Algorithm (GA)-based solutions. Particle Swarm Optimization (PSO) is a randomized optimization algorithm based on the social behaviour of bird flocks/fish schooling. Each solution in PSO is a 'bird' in the search space. Each particle has a strength value that is computed by the fitness function is evaluated and a velocity that describes the element's movement [12].

The elements float through the search space, adjusting their velocities dynamically based on their previous actions [13]. This method directs the elements in the search space to an improved search area. Because of the mobility of the components and the lack of centralised control in MANET, delivering packets from source to destination is problematic. The swarm intelligence approach can be used to tackle these challenges. Kennedy and Eberhart (1995) first proposed the PSO algorithm in terms of social and cognitive behaviour [14]. Multi-hop clustering with load-balancing features is called adaptive multi-hop clustering. Each mobile node sends its node ID, Cluster Head ID, and State (Cluster Head (CH)/Cluster Member (CM) /Gateway) to other mobile nodes in the cluster regularly. Each mobile node receives data about its cluster's topology via this transmission [15]. Each gateway also communicates with other gateways in various clusters regularly and reports to the CH. As a result, CH determines the number of mobile nodes in each nearby cluster. Adaptive Multi-hop Clustering (AMC) establishes Upper and Lower boundaries (U/L) on the respective CMs, which every CH could manage within a cluster.

3 Proposed Methodology

3.1 Attacks on Dynamic Source Routing

Due to their mobility of nodes, MANETs are dynamic networks that are used as multi-hop networks. Routing is the process of sending packets to their endpoints via the most efficient route. The effectiveness of a route is determined by various factors, including the number of hops, network traffic, and authentication. All hosts in MANETs function are specialised routers. Attacks in MANET can be categorised by their source, external/internal, and their behaviour, which can be passive/active. External attacks are launched by nodes which is not connected to the network, and internal threats are initiated by network nodes that are either compromised or malfunctioning [16–20].

Instead of sending packets, blackhole attacks discard them entirely. A misbehaving node may be either selfish/malicious. Selfish nodes don't participate in routing operations and discard packets to save battery power/Central Processing Unit (CPU) cycles. Malicious nodes drop the packets, modify routing data, and masquerade as other nodes to disrupt network functionality and accessibility. A blackhole attack occurs when nodes selectively drop packets instead of discarding all packets of a specific node/at predetermined intervals [21,22].

The method by which malicious nodes are integrated into the data route may vary. Fig. 1 depicts the development of the blackhole challenges. If Node **A** wants to send a data packet to Node **D**, it initiates the route discovery method. As Node **C** is malevolent, it establishes an active path to the endpoint as soon as it has Route Request (RREQ). It then sends a response to Node **A** before sending it to other nodes. As a result, Node **A** considers this an active path, and route discovery is completed. Node **A** then starts sending data packets to Node **C**, disregarding all other Route Reply (RREP).

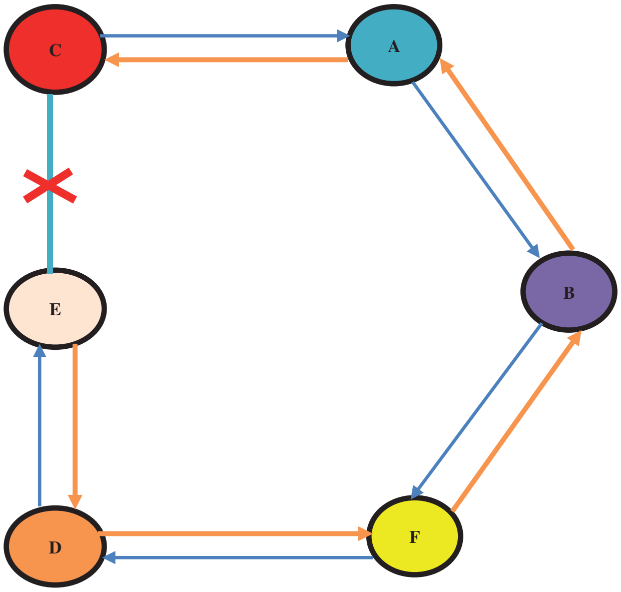


Figure 1: Model of attacks in MANET

DSR protocols are efficient routing protocols designed for multi-hop MANETs with mobile nodes. DSR is an on-demand/reactive routing mechanism. This protocol was created to decrease the size of bandwidth loss in MANET due to control packets and to eliminate the table-driven systematic approach. When DSR is used, MANETs are completely self-configuring and do not require any network design. Nodes in a network coordinate and send packets for each other, allowing transmission over multi-hops among nodes which is not in the wireless connectivity range of one another [23–29].

Because the number of intermediate hops necessary to reach a target may vary, the resulting network topologies are diverse and dynamic. End-to-End Acknowledgments have been utilised in a variety of MANET methods to identify malicious routing activities. The idea of the 2-ACK method is that when nodes exchange data packets over the next hop, the next hop's destination node-link sends back a 2-hop ACK termed 2-ACK that signifies PDR. ACK packets on the Medium Access Control (MAC)/Transmission Control Protocol (TCP) levels are compared with 2-ACK packets. 2-ACK addresses the issues of ambiguity collision, receiver collisions, and transmitted power limitations. The approaches, though, result in higher control overheads but are not suitable for MANETs.

In MANETs, the effect of a blackhole attack can be seen. The obtained experimental comprises 50 nodes spread out over a 2 *km* area. There were two tests: one with no harmful nodes and one with malicious nodes accounting for 10% to 50% of the nodes. The simulated setup is listed in Tab. 1, and the Packet Delivery Ratio (PDR), Control Packet Overhead (CPO), and End-to-End Delay (EED) for MANET are shown in Figs. 2–4.

Table 1: Simulation setup

Simulations parameters	Value
Data transmission rate	2 Mbps
Transmit power	50 mW
Node power threshold	−95 dBm
Node mobility speed	5 ms
Route time out	4 s
Hello message interval	Uniform

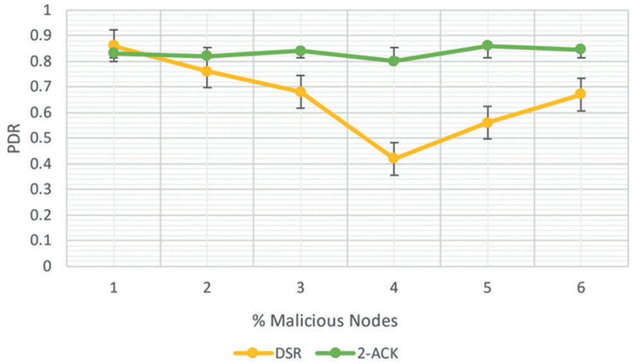


Figure 2: PDR in MANET DSR *vs.* 2-ACK

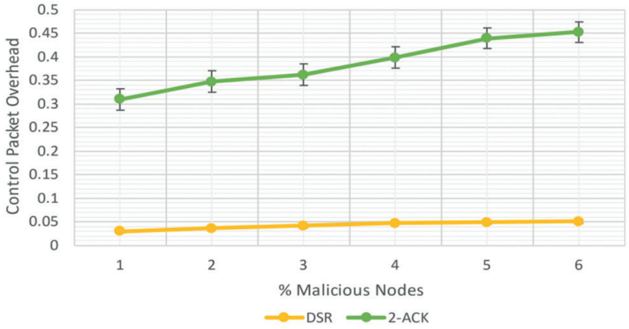


Figure 3: CPO in MANET DSR *vs.*2-ACK

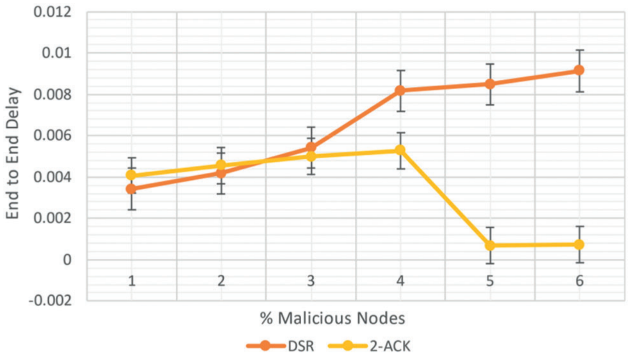


Figure 4: EED in MANET for DSR *vs.* 2-ACK

3.2 Simulation Performance Results in MANET

The PDR of 2-ACK is 3.5% lower than DSR at 0% malicious node, as shown in Fig. 2. At the same time, the PDR of 2-ACK outperforms DSR by 62.3% at 30% malicious node.

As shown in Fig. 3, the PO of 2-ACK improved by 161.3% to DSR at 0% malicious node. Comparable to DSR, the PO of 2-ACK increased by 152% at 30% malicious node.

As shown in Fig. 4, the EED of 2-ACK is 17% than DSR at 0% malicious node. However, for 30% of malicious nodes, the EED of 2-ACK delay is 43% lesser than DSR. 2-ACK performed best when the level of maliciousness rises. As the network's maliciousness grows, the PDR for DSR drops dramatically. In addition, as the level of maliciousness rises, the EED of DSR rises as well.

4 Cluster Trust Adaptive Acknowledgment Routing

Because of the dynamic architecture of MANET, routes connecting two separate nodes likely fail due to mobility. As a result, in order to enhance MANET versatility and prevent rerouting, security procedures have little computation time . For MANETs, security is critical, particularly for real-time applications. We evaluate various features while securing a MANET: Accessibility, Privacy, integrity, Authenticity, and Non-repudiation. The continual mobility of nodes is one of the primary difficulties for MANET Routing, and the intermediate node movement in the routing path and end nodes leads to disruption and frequent path breaks. For routing protocols in MANETs, effective mobility for dynamic MANETs should be a key component.

IDS is a method that captures data from systems that need to be protected. It makes use of three categories of data: long-term data connected with IDS methods that make use of the attacker's understanding base's skill, configuration data about the present system state, and audit data that specifies system occurrences. Detectors exclude non-essential data from audit trails and give synthesized representations of security-related activities. Decisions are made based on certain activities/situations and may interpret as an intrusion detection/vulnerability. The countermeasure component ensures that corrective actions are taken to prohibit actions from being executed or return the system in secured manner. Fig. 5 shows an example of IDS.

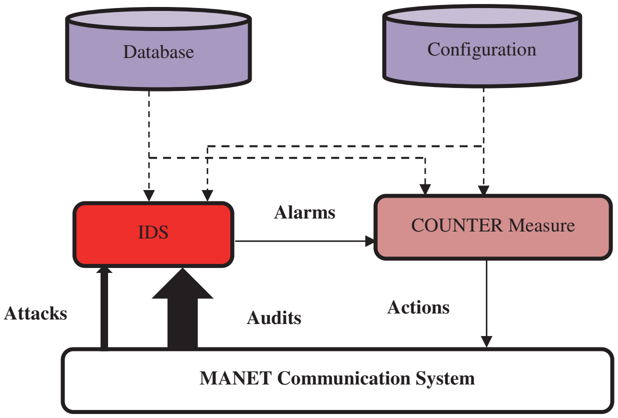


Figure 5: An IDS for MANET

The acknowledge packets are also used in the Adaptive Acknowledge (AACK) System. The network overhead generated by acknowledgement packets in the above method can be decreased by employing the AACK approach. The End-to-End Acknowledgement system and the Enhanced 2-ACK method are combined to form the AACK. To minimize network load overhead and to identify harmful network nodes, the Cluster Trust Adaptive Acknowledgment (CTAA) approach is deployed (Fig. 6).

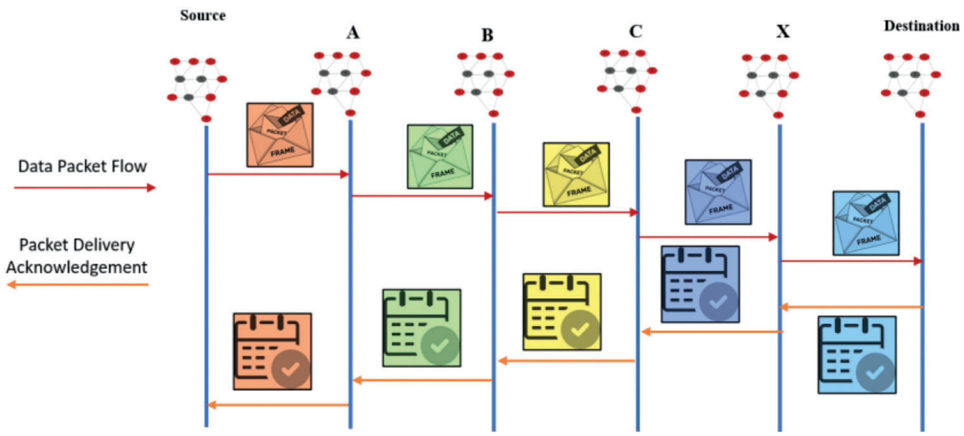


Figure 6: Cluster Trust AACK

It has the ability to use a cluster-based routing protocol as well as an advanced AACK method. Each cluster inside the network can implement an upgraded AACK system in their local area to identify misbehaving nodes, restricted transmitted node power issues, and other collision issues inside the node. After detecting malicious nodes inside each network, the transferred data between the two separate nodes correspond to the same/different cluster.

It can transfer data through multi-hops belonging to various clusters using the simple End-To-End acknowledgement technique described earlier. This enhanced ID help to prevent fake misbehaving reports as well as other intrusion issues. It could also prevent acknowledgement packet forgery by drastically reducing the number of acknowledgement packets sent; it can easily identify malicious nodes prior to delivering data; thus, acknowledgement packet forgery must not exist in the MANET.

The present CH may regulate the presence and dismissal of nodes; therefore, network performance is unaffected. In comparison to other IDS, the network's PDR and performance could be higher. In CTAA, the idea of adopting a hybrid strategy effectively decreases overhead. As a result, the proposed CTAA detects malicious nodes while lowering network overhead.

4.1 Kalman Filter

To minimize noise and delay, KF uses an x̃-based method. Robust time synchronization against the node mobility in a MANET is obtained using both median-based techniques and KF. Fig. 7 shows x̃ in the n^{th} synchronization round, where, $Node_T$ is the n^{th} synchronization round's start time, blue lines are obtained logical clocks, and orange lines are calculated logical clocks at the synchronization round boundary.

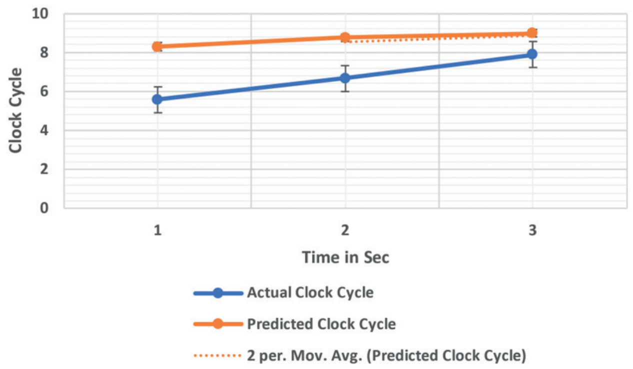


Figure 7: Time synchronization in KF

4.2 Algorithm of Kalman Filter

```
Step 1. Set Threshold Limit of $\tilde{x}$
Step 2. **For Each** $j \in Node_i$
Step 3. {
Step 4. $Lj(t(Node+1)) = Lj(t_{node})+(Hi(t(Node+1))-Hi(t_{node}))\times Rij(t_{node})\times lj$
Step 5. {
Step 6. **End For**
Step 7. $v \in Node_i$ $(Lv(t(Node+1)))$
Step 8. $M = \tilde{x}v \in Node_i(Lv(t(n+1))$
Step 9. **For Each** $j \in Ni$
Step 10. $e = LM(t(k+1))-Lj(t(k+1))$
Step 11. **If** $e <$ Threshold Value **Then**
Step 12. **{**
Step 13. $\tilde{x} = j$;
Step 14. }
Step 15. **End If**
Step 16. **End For**
Step 17. **End**
```

The $\overline{\overline{X}}$ process is used by KF to eliminate possible errors by topological changes/randomization in transmitting and receiving data. The input to the KF can be stated as Eqs. (1) and (2) If $Node_i$ selects $Node_j$ as a $\overline{\overline{X}}$ node.

$$Node_T = LCR_i(Node_n) - LCR_j(Node_n) \tag{1}$$

$$Route_n = \frac{x_j(Node_T) - x_i(Node_T)}{x_i(Node_T)} = \frac{LCR_i(Node_n) - LCR_j(Node_{n-1})}{LCR_i(Node_n) - LCR_i(Node_{n-1})} = \frac{Route_{i,j}LCR_j}{LCR_i} - 1 \tag{2}$$

In the i^{th} round, $Node_T$ is the logical clock variation between $Node_i$ and $Node_j$. The absolute Logical Clock Rate (LCR) differential between $Node_i$ and $Node_j$ is divided by the absolute LCR of $Node_i$ in the n^{th} round to get $Route_n$. As seen in, $Node_{\mathrm{x}}$ is a column vector with the elements $Node_T$ and $Node_R$, Eq. (3)

$$Node_x = \frac{Node_{Total}}{Route_N} \tag{3}$$

where, $Node_X$ denotes the actual values in the i^{th} round in a real-world MANET environment.

4.3 Simulation Performance Results of Proposed CTAA

The PDR of suggested CTAA reduced by 2.4% than DSR at 0% malicious performed much better by 1.2% than 2-ACK, represented in Fig. 8. However, the proposed CTAA's PDR outperforms DSR by 63% and 2-ACK by 1.24% malevolent. It is clear that the trusted IDS is operating in a malicious environment.

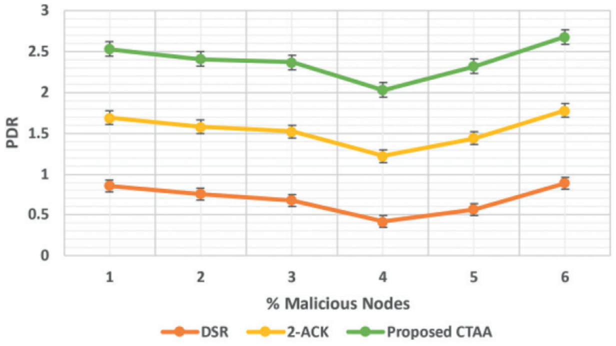


Figure 8: PDR for proposed CTAA

The CPO of suggested CTAA is greater by 161% than DSR and reduced by 107% than 2-ACK at 0% harmful, as shown in Fig. 9. Furthermore, the suggested CTAA's CPO is 152% greater than DSR and 131% less than 2-ACK at 30% malevolent.

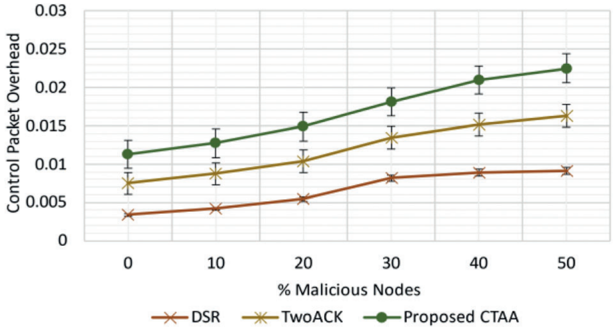


Figure 9: CPO for proposed CTAA

According to Fig. 10, the EED of recommended CTAA is 10.8% lower than DSR at 0% harmful and 6.6% lower than 2-ACK. Therefore, the suggested CTAA has a lower EED of 54.7% compared to DSR and 12.3% compared to 2-ACK, which is 30% harmful.

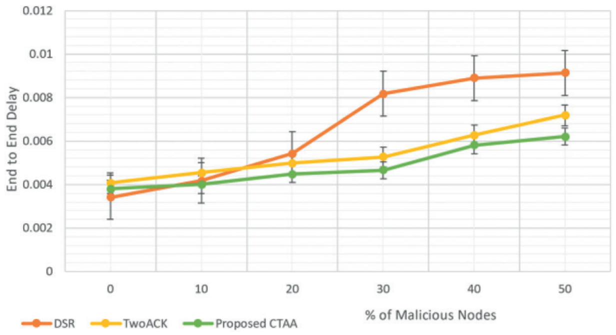


Figure 10: EED for proposed CTAA

5 MOPSO Based Optimized Routing

Kennedy and Eberhart published the PSO algorithm for the first time as a numerical method for frequently optimising challenges; it was associated with the social style of living of birds within a flock, for each bird treated as a particle only within the hyperdimensional search area (Fig. 11). The positioning of the elements in the search area is adaptable and changeable based on the participants' social-psychological tendencies. Two aspects of information/swarm experiences influence elements movement inside the swarm. The way the swarms return to previous successful regions in the solution space results from developing social behaviour. The following Eqs. (4) and (5) are used to solve the Velocity (Node$_v$) of each element as well as the node position (Loc$_x$) of the elements:

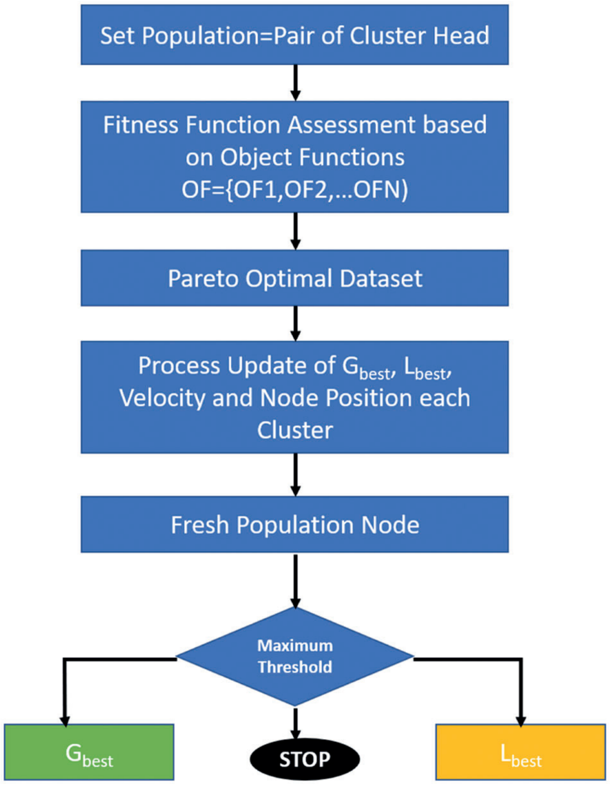

Set Population=Pair of Cluster Head
Fitness Function Assessment based on Object Functions OF={OF1,OF2,...OFN)
Pareto Optimal Dataset
Process Update of G$_{best}$, L$_{best}$, Velocity and Node Position each Cluster
Fresh Population Node
Maximum Threshold
G$_{best}$
STOP
L$_{best}$

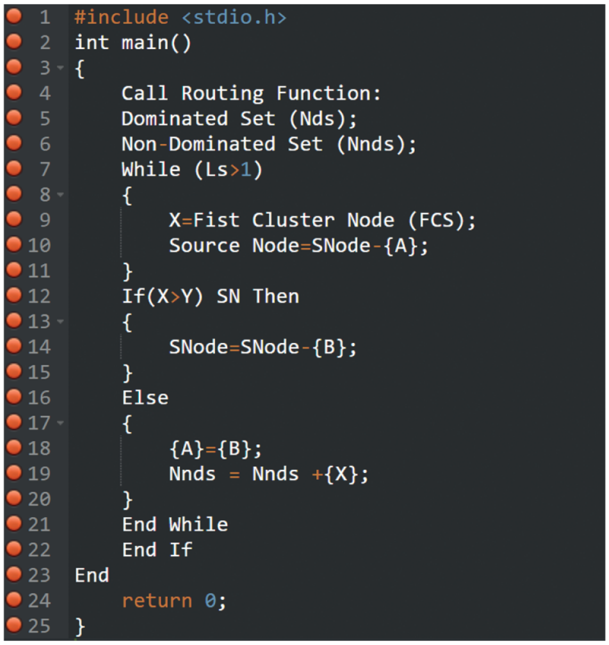
Figure 11: Flowchart of MOPSO routing in MANET

$$Velocity_{i,j}(Time+1) = WeightFactor_{i,j} + LC_1Rnd_1(\Pr obA_{i,j}(Time) - X_{i,j}(Time)) + LC_2Rnd_2(\Pr obB_{i,i}(Time) - X_{i,j}(Time)) \tag{4}$$

$$X_{i,j}(Time+1) = (X_{i,j}(Time) + Velocity_{i,j}(Time+1) \tag{5}$$

where, $Velocity_{i,j}(Time+1)$ indicates element *i's* velocity at iteration *j, $X_{i,j}(Time+1)$* signifies element *i's* position at iteration *j*, and T represents the number of iterations. Furthermore, WF_{ij} is the inertia weight used to minimize the influence of the preceding velocity log. LC_1 is the awareness learning component, LC_2 is the gregarious learning component, and Rnd_1 and Rnd_2 are arbitrary numbers in the solution space between [0,1] for controlling the stored information capacity. To put it another way, to track or erase the immoderate speed by maintaining the component Velocity ($Node_v$) defined with range [$Velocity_{MIN}$, $Velocity_{MAX}$]. The PSO algorithm finds the best position for each element in the swarm. If the number of positions is raised at this point, *i* will not progress. As a result, PSO demonstrates its efficacy and excellence in solving problems.

In the MOPSO algorithm (Fig. 12), the competing method in this research explores the disposal solution set and rapidly creates the external archives set. To begin, choose an element **X** from the population **S**, preferably the first element in the population. Then, using the value of the objective function of Pareto dominance relations, compared with each element in the population using **S = S-{X}**. If **XY**, the element is eliminated from the population **S**; if X = Y, the element remains in the population **S**. Finally, let N = NU{x} until S = Teta, at which point **N** is the nondominant solution set that needs to be rectified. When the nondominant solution set reaches the external archive set, this procedure is used. The number of times the algorithm executes decreases as more elements are eliminated, significantly limiting the method's complexity and increasing its searching performance.



```
#include <stdio.h>
int main()
{
    Call Routing Function:
    Dominated Set (Nds);
    Non-Dominated Set (Nnds);
    While (Ls>1)
    {
        X=Fist Cluster Node (FCS);
        Source Node=SNode-{A};
    }
    If(X>Y) SN Then
    {
        SNode=SNode-{B};
    }
    Else
    {
        {A}={B};
        Nnds = Nnds +{X};
    }
    End While
    End If
End
    return 0;
}
```

Figure 12: The pseudocode of the algorithm

Performance of Proposed Cluster Trust Adaptive Acknowledgement-Multi-Objective Particle Swarm Optimization

The PDR of CTAA-MPSO shows better performance by 3.2% than CTAA-PSO at 0% malicious, as shown in Fig. 13. Similarly, to CTAA-PSO, the PDR of CTAA-PSO outperforms CTAA-PSO by 3.1% at 30% malevolent.

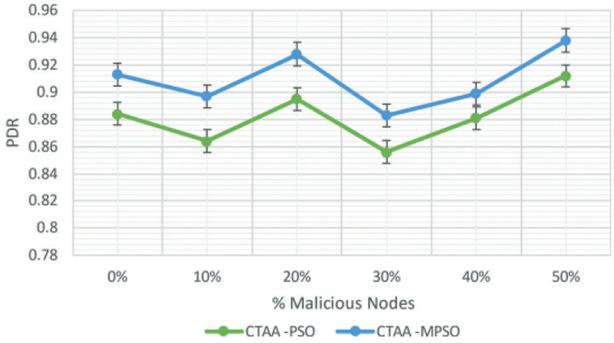


Figure 13: PDR for proposed MPSO

The CPO of CTAA-MPSO is 3.8% lower than CTAA-PSO, which is 0% harmful, as shown in Fig. 14. CTAA-CPO MPSO's is also 3.8% lesser than CTAA-at PSO's.

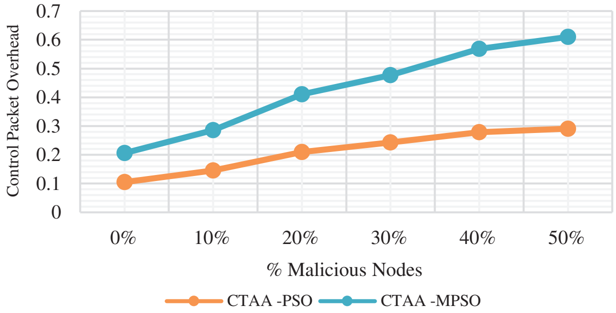


Figure 14: CPO for proposed MPSO

The EED of CTAA-MPSO is 5.5% lesser than CTAA-PSO, which is 0% malicious, as shown in Fig. 15. CTAA-EED MPSO's is also 3.3% lesser than CTAA-at PSO's% harmful. The suggested CTAA-MPSO increases the PDR in MANET. It significantly lowers both CPO and EED.

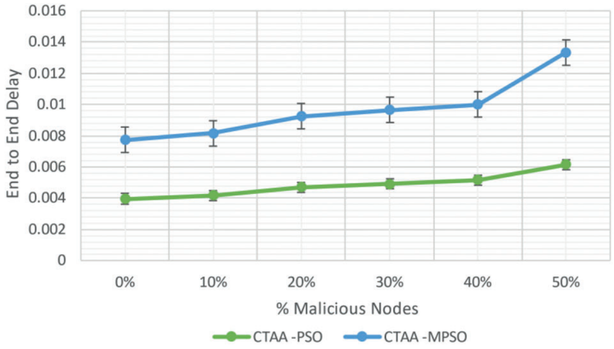


Figure 15: EED for proposed MPSO

6 Conclusion

The success of MANET functions depends on the active nodes' participation in providing a service to one another. Because MANETs allow devices to connect/quit the unauthorized domain, no one node in the domain can be guaranteed. In MANET, the effect of a blackhole attack is assessed. The new IDS Enhanced CTAA approach addresses many issues that have plagued prior IDS, such as false misbehaving reports and network overhead caused by many acknowledged packets. In this paper, the researcher offers a time synchronisation algorithm for mobile contexts that uses the Median synchronisation message to exclude outliers and KF to decrease synchronisation errors. We offer a multi-objective approach in this research that uses the MOPSO algorithm to optimise the number of clusters in an ad hoc network and energy loss in nodes to give an energy-efficient method and decrease network traffic. At 0% malicious node, 2-ACK's PDR outperforms DSR by 3.5%. Likewise, the PDR of 2-ACK outperforms the DSR for MANET by 62.3% at 30% malicious node. Methods to reduce the consequences of a blackhole attack

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Achankunju, R. Pushpalakshmi and A. V. A. Kumar, "Particle swarm optimization based secure QoS clustering for mobile ad hoc network," in *IEEE Int. Conf. on Communication and Signal Processing*, Melmaruvathur, India, pp. 315–320, 2013.

[2] K. M. Omran, "The routing control in mobile Ad hoc network using intelligent optimization algorithms," in *Int. Conf. on Electrical, Communication, and Computer Engineering (ICECCE)*, Istanbul, Turkey, pp. 1–6, 2020.

[3] N. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf and M. Irfan, "Mobile ad-hoc networks applications and its challenges," *Communications and Network*, vol. 2016, no. 8, pp. 131–136, 2016.

[4] J. J. Liang, A. K. Qin, P. N. Suganthan and S. Baskar, "Comprehensive learning particle swarm optimizer for global optimization of multimodal functions," *IEEE Transactions on Evolutionary Computation*, vol. 10, no. 3, pp. 281–295, 2006.

[5] X. Guo, S. Yang, L. Cao, J. Wang and Y. Jiang, "A new solution based on optimal link-state routing for named data MANET," *China Communications*, vol. 18, no. 4, pp. 213–229, 2021.

[6] H. Jhajj, R. Datla and N. Wang, "Design and implementation of an efficient multipath AODV routing algorithm for MANETs," in *IEEE 9th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, pp. 0527–0531, 2019.

[7] I. Alameri, J. Komarkova and M. K. Ramadhan, "Conceptual analysis of single and multiple path routing in MANET network," in *Int. Conf. on Information and Digital Technologies (IDT)*, Zilina, Slovakia, pp. 235–244, 2021.

[8] S. U. Masruroh, A. Z. S. Perdana, H. B. Suseno, A. Fiade, D. Khairani *et al.,* "Energy efficient routing protocol AOMDV on MANET (Mobile Ad-hoc network) with malicious node," in *5th IEEE Int. Conf. on Informatics and Computing (ICIC)*, Gorontalo, Indonesia, pp. 1–4, 2020.

[9] F. Semchedine, A. Moussaoui, K. Zouaoui and S. Mehamel, "CRY OLSR: Crypto Optimized Link State Routing for MANET," in *5th Int. Conf. on Multimedia Computing and Systems (ICMCS)*, Marrakech, Morocco, pp. 290–293, 2016.

[10] B. Han, L. Ding, Y. Ji, X. Wang and B. Wang, "A TORA-based wireless protocol for MANET with low routing overhead at link layer," in *IEEE 17th Int. Conf. on Mobile Ad Hoc and Sensor Systems (MASS)*, Delhi, India, pp. 283–291, 2020.

[11] S. Sudhakar, O. I. Khalaf, P. Vidya Sagar, D. K. Sharma, L. Arokia Jesu Prabhu *et al.,* "Secured and privacy-based IDS for healthcare systems on e-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–11, 2022.

[12] S. Sudhakar, O. I. Khalaf, G. R. K. Rao, D. K. Sharma, K. Amarendra *et al.,* “Security-aware routing on wireless communication for e-health records monitoring using machine learning,” *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–10, 2022.

[13] S. Sudhakar, O. I. Khalaf, S. Priyadarsini, D. K. Sharma, K. Amarendra *et al.,* “Smart healthcare security device on medical IoT using raspberry Pi,” *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–11, 2022.

[14] S. Sudhakar, G. R. K. Rao, O. I. Khalaf and M. Rajesh Babu, “Markov mathematical analysis for comprehensive real-time data-driven in healthcare,” *Mathematics in Engineering Science and Aerospace (MESA)*, vol. 12, no. 1, pp. 77–94, 2021.

[15] S. Sudhakar, P. Vidya Sagar, R. Ramesh, O. I. Khalaf and R. Dhanapal, “The optimization of reconfigured real-time datasets for improving classification performance of machine learning algorithms,” *Mathematics in Engineering Science and Aerospace (MESA)*, vol. 12, no. 1, pp. 43–54, 2021.

[16] R. Vasanthi, O. I. Khalaf, C. A. T. Romero, S. Sudhakar and D. K. Sharma, “Interactive middleware services for heterogeneous systems,” *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1241–1253, 2022.

[17] A. Mehbodniya, S. Bhatia, A. Mashat, E. Mohanraj and S. Sudhakar, “Proportional fairness based energy-efficient routing in wireless sensor network,” *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1071–1082, 2022.

[18] D. Stalin David, S. Arun Mozhi Selvi, S. Sivaprakash, P. Vishnu Raja, D. K. Sharma *et al.,* “Enhanced detection of glaucoma on ensemble convolutional neural network for clinical informatics,” *Computers, Materials & Continua*, vol. 70, no. 2, 2022, pp. 2563–2579, 2022.

[19] D. Stalin David, M. Anam, K. Chandraprabha, S. Arun Mozhi Selvi, D. K. Sharma *et al.,* “Cloud security service for identifying unauthorized user behaviour,” *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2581–2600, 2022.

[20] K. Rajakumari, M. Vinoth Kumar, G. Verma, S. Balu, D. K. Sharma *et al.,* “Fuzzy based ant colony optimization scheduling in cloud computing,” *Computer Systems Science and Engineering*, vol. 40, no. 2, pp. 581–592, 2022.

[21] R. Nithya, K. Amudha, A. Syed Musthafa, D. K. Sharma, E. H. Ramirez-Asis *et al.,* “An optimized fuzzy-based ant colony algorithm for 5G-MANET,” *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1069–1087, 2022.

[22] S. Sudhakar and S. Chenthur Pandian, “Secure packet encryption and key exchange system in mobile ad hoc network,” *Journal of Computer Science*, vol. 8, no. 6, pp. 908–912, 2012.

[23] S. Sudhakar and S. Chenthur Pandian, “Hybrid cluster-based geographical routing protocol to mitigate malicious nodes in mobile ad hoc network,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 21, no. 4, pp. 224–236, 2016.

[24] A. U. Priyadarshni and S. Sudhakar, “Cluster based certificate revocation by cluster head in mobile ad-hoc network,” *International Journal of Applied Engineering Research*, vol. 10, no. 20, pp. 16014–16018, 2015.

[25] S. Sudhakar and S. Chenthur Pandian, “Investigation of attribute aided data aggregation over dynamic routing in wireless sensor,” *Journal of Engineering Science and Technology*, vol. 10, no. 11, pp. 1465–1476, 2015.

[26] S. Sudhakar and S. Chenthur Pandian, “Trustworthy position based routing to mitigate against the malicious attacks to signifies secured data packet using geographic routing protocol in MANET,” *WSEAS Transactions on Communications*, vol. 12, no. 11, pp. 584–603, 2013.

[27] S. Sudhakar and S. Chenthur Pandian, “A trust and co-operative nodes with affects of malicious attacks and measure the performance degradation on geographic aided routing in mobile ad hoc network,” *Life Science Journal*, vol. 10, no. 4s, pp. 158–163, 2013.

[28] S. Sudhakar and S. Chenthur Pandian, “An efficient agent-based intrusion detection system for detecting malicious nodes in MANET routing,” *International Review on Computers and Software (I.RE.CO.S.)*, vol. 7, no. 6, pp. 3037–304, 2012.

[29] S. Sudhakar and S. Chenthur Pandian, “Authorized node detection and accuracy in position-based information for MANET,” *European Journal of Scientific Research*, vol. 70, no. 2, pp. 253–265, 2012.