Development of Trust metrics using Swarm Intelligence Techniques for Mobile Adhoc Networks

Mogaji Stephen Alaba, Alese Boniface Kayode, Adetunmbi, Adebayo.O., Olabode, Olatubosun
alabadepoola@yahoo.com, bkalese@futa.edu.ng, bayoadetunmbi@gmail.com, olabode_olatubosun@yahoo.co.uk
School of Computing, Federal University of Technology Akure. Nigeria.

Abstract: Trustworthiness evaluation has become a significant issue in securing network environments to allow participating network nodes decide on the reliability and trustworthiness of other nodes before generating a communication channel
Swarm Intelligence (SI) is a relatively new paradigm being applied in a host of research settings to improve the management and control of large numbers of interacting entities such as communication, computer networks, satellite constellations and more.
This research work proposes different approaches to evaluate the trustworthiness of Mobile Adhoc Networks using swarm intelligence methodology and designing trust metrics that are computed using multiple properties of trust and quality of service.
An improved swarm intelligence algorithm is proposed for this purpose by hybridizing the conventional Particle Swarm Optimization (PSO) algorithm with the pheromone mechanism of Ant Colony Optimization (ACO). The proposed model is then benchmarked against standard optimization test functions.
A trust metric objective function is designed to determine trustworthiness of nodes using the proposed hybridized model.
The model is then simulated using a NS-2. The effect of evaluating trustworthiness and discovering misbehaving nodes prior to interactions, as well as their influence on the network performance were carried out.

Index terms: Swarm Intelligence, Mobile Adhoc Networks, Trustworthiness, Pheromone-guided mechanism, Honesty, Confidence, Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Hybridization.

---

1. INTRODUCTION

Applying swarm behavior in computing environments as a novel approach is appeared to be an efficient solution to face critical challenges of the modern cyber world
In the past few years biology based techniques get the attentions of researchers in the field of Information Security.
These and other phenomena inspired researchers to study and understand their secrets. The unraveling of many of these mysteries and secrets led to the foundation of new artificial intelligence science known as Swarm Intelligence (SI).

n is needed and the process of assigning and evaluating the important parameters should be introduced.
Thus based on such intelligent behavior of swarms various algorithms have been designed. Swarm intelligence is a modern artificial intelligence discipline that is concerned with the design of multi-agent systems with applications, for example, in optimization and in robotics. The design paradigm for these systems is fundamentally different from more traditional approaches. Instead of a sophisticated controller that governs the global behavior of the system, the swarm intelligence principle is based on many unsophisticated

A swarm is a large number of homogenous, simple agents interacting locally among themselves, and their environment, with no central control to allow a global interesting behavior to emerge.
. Swarm intelligence is the emergent collective intelligence of groups of simple agents. It is a computational intelligence approach to solve real world complex problems.
Simulation is one of the best processes to monitor the efficiency of each system's functionality before its real implementation. Because of the novel and special nature of swarm-based systems, a clear roadmap toward swarm simulatio
entities that cooperate in order to exhibit a desired behavior. Inspiration for the design of these systems is taken from the collective behavior of social insects such as ants, termites, bees, and wasps, as well as from the behavior of other animal societies such as flocks of birds or schools of fish.

2. SWARM INTELLIGENCE IN MANETS

The concept of Swarm intelligence is an interesting one and it is designed based on the following analogies.

i. Distributed system of interacting autonomous agents.
ii. Goals: performance optimization and robustness.
iii. Decentralized: Self-organized control and cooperation
iv. Division of labor and distributed task allocation.
v. Indirect interactions

It is found that the Swarm Intelligence (SI) inspired algorithms such as Ant Colony Optimization (ACO) are better suited for highly adaptive networks like Mobile Ad hoc Networks (MANETs) [39]. Biological ants at the time of food foraging, navigate their chosen path and deposit a chemical called pheromone on the ground, there by establishing the trail. Thickness of the trail attracts other ants to follow the path to reach the food source.
Mobile Ad-hoc Network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. It is a set of wireless communication nodes performing self-configuration in a dynamic mode for formation of network excluding fixed infrastructure or centralized supervision. Often, there may be random changes in the network topology as nodes are mobile. In addition to the role of router, the nodes also play the role of end host. The routing protocol in such a network is an authority to determine the routes and offering communication among end points via intermediate nodes. The MANET is well liked and attractive since they offer good communication in the changing infrastructure for the applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like.

The objectives of this paper are to hybridize Particle Swarm Optimization (PSO) using the pheromone mechanism of Ant Colon Optimization (ACO), design a model based on proposed hybridized swarm intelligence concept for trust management in MANETS using multidimensional social trust metrics and Quality of Service (QoS) and implement the proposed model in a simulated Mobile Ad-hoc Network (MANET) environment.

3. RELATED LITERATURES

He, et.al [18] proposed a reputation-based trust management scheme using an incentive mechanism, called SORI (Secure and Objective Reputation-based Incentive). This scheme encourages packet forwarding and discourages selfish behaviors based on quantified objective measures and reputation propagation by a one-way hash chain based authentication.
The performance of this scheme in the presence of malicious nodes, as may be expected in a hostile environment, has not been investigated.

Yonfang [50] suggests two different approaches to evaluate trust: policy-based trust management and reputation-based trust management. Policy-based approach is based on strong and objective security schemes such as logical rules and verifiable properties encoded in signed credentials for access control of users to resources. Such a policy-based trust management approach usually makes binary decision according to which the requester is trusted or not, and accordingly the access request is allowed or not. Due to the binary nature of trust evaluation, policy-based trust management has less flexibility. On the other hand, reputation-based trust management utilizes numerical and computational mechanism to evaluate trust. Typically, trust is calculated by collecting, aggregating, and disseminating reputation among the entities.

Nekkanti and Lee [30] extended AODV (Ad hoc On demand Distance Vector) using trust factor and security level at each node. Their approach deals differently with each route request based on the node's trust factor and security level.
In a typical scheme, routing information for every request would be encrypted leading to large overheads; they propose to use different levels of encryption based on the trust factor of a node, thus reducing overhead. This approach adjusts the security level based on the recognized hostility level and hence can conserve resources; however, the approach does not treat evaluation of trust itself

4. SYSTEM DESIGN

Swarm intelligence meta-heuristics, namely, particle swarm optimisation and ant colony optimisation are proven to be successful approaches to solve complex optimization problems. PSO algorithm, whose concept began as a simulation of a simplified social environment, is a powerful optimization technique for solving multimodal optimization problems [30], [6], [31]. ACO imitates foraging behaviour of real life ants, and are known to be efficient and robust for solution of combinatorial optimization problems [40], [6], [49], [44].

The implementation of this proposed algorithm comes in two stages. In the first stage, PSO is applied while ACO is implemented in the second stage. ACO works as a local search, wherein, ants apply pheromone-guided mechanism to update the positions found by the particles in the earlier stage, to attain rapid convergence on a feasible solution space. The implementation of ACO in the second stage of this model is based on the studies of Angeline [1] which shows that:

i. PSO discovers reasonable quality solutions much faster than other evolutionary algorithms
ii. If the swarm is going to be in equilibrium, the evolution process will be stagnated as time goes on. Thus, PSO does not possess the ability to improve upon the quality of the solutions as the number of generations is increased.

In this proposed model, a simple pheromone-guided mechanism of ACO is proposed to apply as local search.

The proposed ACO algorithm handles P ants equal to the number of particles in PSO. Each ant i generates a solution zt around gbest the global best-found position among all particles in the swarm up to iteration count t as [41].

$$z_t = N(g_{best}, \sigma) \quad (1)$$

The components of the solution vector z_t which satisfies the Gaussian distribution with mean g_{best} and standard deviation σ is generated, where, initially at t = 1 value of σ = 1 and is updated at the end of each iteration as

$$\sigma = \sigma \times d \quad (2)$$

d is a parameter in (0.25, 0.997) and if $\sigma < \sigma_{min}$ then $\sigma = \sigma_{min}$, where, σ_{min} is a parameter in (10-2 , 10-4).

The objective functions aroundz_t, $f(z_t)$ is the computed and replaces the current position of the particle swarm if $f(z_t) < f(x_t)$ then

$$x_t = z_t \quad (3)$$

This simple pheromone-guided mechanism considers there is highest density of trails (single pheromone spot) at the global best solution gbest of the swarm at any iteration t + 1 in each stage of ACO implementation and all ants P search for better solutions in the neighbourhood of the global best solution. In the beginning of the search process, ants explore larger search area in the neighborhood of gbest due to the high value of standard deviation r and intensify the search around gbest as the algorithm progresses [41]. ACO pheromone mechanism helps PSO process, not only to efficiently perform global exploration for rapidly attaining the feasible solution space, but also to effectively reach optimal or near optimal solution.

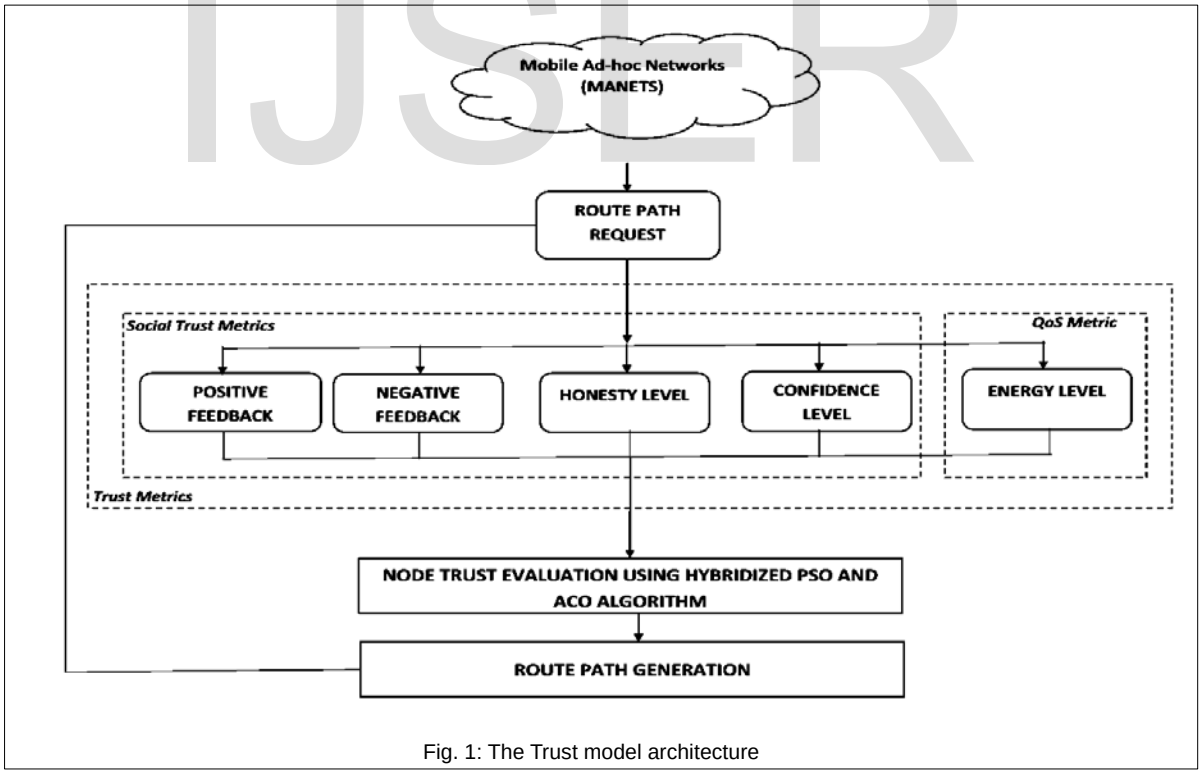

Fig. 1: The Trust model architecture

In this research, Social and QoS properties are considered to evaluate trustworthiness of nodes while the proposed hybridized optimisation algorithm enhances accuracy by ensuring that the shortest trusted path is chosen resulting into a positive impact on improving network performance. Metrics

associated with the formulation of nodes trustworthiness are described below.

4.1 Positive Interaction

In MANETS, positive interaction (or feedback) is a social factor, referred to as the accumulated number of forwarding packets successfully delivered by a node in the network. This value is represented as ρ. Accumulated positive interaction is calculated as

$$\alpha = \rho + 1. \quad (4)$$

4.2 Negative Interactions

In contrast to positive feedbacks, negative interaction is an important social factor described as the number of packets dropped by a node on the network. This value is represented as n. Accumulated negative interaction, β is calculate as

$$\beta = n + 1. \quad (5)$$

4.3 Honesty

Honesty is a social property and a friendship-based trust model metric, which is defined as the way in which nodes behave in terms of acting to favour themselves or the communities of which they are a part of [2]. Honesty is an important social trust factor in the proposed model and it refers to the degree of honesty of the evaluating node about the evaluated node i. It is a measure of successful or failed interactions.

Negative and positive behaviours of nodes are indicators of the honesty of nodes in detecting irregular behaviour. The value of Honesty, $T_{ij}^{honesty}$ is computed by using the number of successful interactions α_{ij} between node i and j over the maximum number of successful and failed interactions$\alpha_{ij} + \beta_{ij}$.

$$T_{ij}^{honesty} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \quad (6)$$

The initial value of $T_{ij}^{honesty}$ is 0.5 at time t = 0, which means that node i is a stranger to node j and no previous interaction has been observed. $T_{ij}^{honesty}$develops over time also, and its value is between 0 and 1. Positive interactions increase the value of honesty while negative interactions can lead to a decrease in its value.

4.4 Confidence Metric

Confidence is another friendship-based trust metric [35] and an important social property that is used to indicate how strong a tie is between two interacting nodes. It measures how frequently nodes interact with one another to evaluate relationship strength between interacting nodes. Basically, it evaluates the number of interaction between nodes. A high number of interactions can be translated into the idea that the evaluating node has a strong relationship with the evaluated node. Consequently, it improves the ability of the evaluating node to judge the trustworthiness of the node under evaluation.

Confidence $T_{ij}^{confidence}$ is expressed as the variance value of all past experiences between two interacting nodes. Its value is measured by using the beta standard deviation σ

$$T_{ij}^{confidence} = 1 - \sqrt{12\sigma_{ij}} \quad (7)$$

$$\sigma_{ij} = \frac{\alpha_{ij} \times \beta_{ij}}{(\alpha_{ij} + \beta_{ij})^2 + (\alpha_{ij} + \beta_{ij} + 1)} \quad (8)$$

Beta standard deviation equation is redefined to normalise its values on the interval [0, 1] using the constant $1 - \sqrt{12\sigma_{ij}}$. α_{ij} and β_{ij} represents the positive and negative interaction observed by node i and j. When time t = 0 node i is not able to judge the honesty of node j even if its honesty value is more than a trust threshold, α_{ij} and β_{ij} is 1 and $T_{ij}^{confidence}$ = 0. Confidence develops overtime by increasing the number of positive or negative interactions. The updated value of α_{ij} and β_{ij} will be calculated as $\alpha_{ij} = \rho + 1$ and $\beta_{ij} = n + 1$, where ρ and n represent the positive and negative collected observations respectively, and ρ and n ≥ 0 [35].

4.5 Energy Level

Energy is a critical Quality of Service (QoS) factor in trust systems. All nodes are energy-constrained and the lifetime of each node depends on its energy consumption. In the proposed model, the Energy Level, EV_{ij} factor indicates the remaining energy level of the node after each trust update interval t performed by the evaluating node i about the evaluated node j. The energy factor is calculated as

$$EV_{ij} = \frac{EV_{ij}^{Current} - EV_{ij}^{Consumed}}{EV_{ij}^{Initial}} \quad (9)$$

Where

- $EV_{ij}^{Consumed}$ is the level of energy consumed by node j in performing interactions
- $EV_{ij}^{Current}$ is the previous current energy of node j

- $EV_{ij}^{Initial}$ is the initial level of energy of node j to start with.

Energy is initially at the same level for all nodes in the network. Receiving and transmitting packets are the only types of communications which are considered for energy consumption. Over time, the level of energy is adjusted based on each node's interactions. The value of the energy factor is defined in the interval [0, 1]. It starts at 1, which refers to a situation where nodes have a full battery, and gradually decreases over time as nodes involve themselves in more communications. Nodes continue to be effective in performing interactions so long as the energy factor is not reduced to a particular threshold

4.6 Trust Model Objective Function for Hybridized Algorithm

In the proposed system algorithm, the objective function, also referred to as the fitness function or cost function, is the performance index of particles in the population. In this work, the objective function represents the evaluated trustworthiness in generating a trusted routing path.
To generate a routing path between a source node and a destination node, trustworthiness of intermediate nodes are evaluated to ascertain that constraints are met, social trust and quality of service requirements are fulfilled. When the trust value or cost value is bigger, the performance is better.
The cost function is evaluated using multidimensional social trust and QoS metrics describes above. The social trust metrics are positive interaction, negative interaction, honesty and confidence level, while the energy factor represents an important QoS metric. The trustworthiness is therefore evaluated by combining all metrics. The confidence factor, $T_{ij}^{confidence}$, measures the level of experience between interacting nodes. The honesty factor, $T_{ij}^{honesty}$, measures selfishness or maliciousness of nodes. The energy factor, EVij, measure if a node is capable of performing an intended task or not. The threshold for all multidimensional metrics introduced in this work is 0.5

$$T_{ij} = \frac{T_{ij}^{honesty} + T_{ij}^{confidence} + EV_{ij}}{3} \quad (10)$$

5. SYSTEM IMPLEMENTATION

The hybridized PSO algorithm and standard PSO algorithm is experimented on 50 particles in solution space over 100 iterations. The inertia weight is set as 1.0 and the cognitive parameter, c1, and social parameter, c2 are taken as 2.0. The model is then applied in a simulated MANET environment with specialized configurations and a detailed analysis of the simulation is presented.

In order to generate a routing path between a source and the destination node, trustworthiness of intermediate nodes are evaluated. When the trust value or cost value is higher, the better the performance of the proposed system.

The trustworthiness T_{ij} is therefore evaluated by combining all metrics setting the threshold for all multidimensional metrics to 0.5, any node whose Trust value or cost value is evaluated to be less than the set threshold which is 0.5 is considered to be malicious or misbehaving node

5.1 The Network Simulator

There are many tools available for simulations of network topologies. But the proposed algorithm is simulated using the Network Simulator 2 (NS-2) tool.

NS-2 is an open-source discrete event simulator designed mainly for networking research. NS-2 is an event driven packet level network simulator developed as part of the VINT project (Virtual Internet Testbed).

6. EXPERIMENTAL SETUP

A network with 50 randomly placed nodes is simulated. Several nodes were randomly selected to be misbehaving by dropping packets by different rates. Table 1 shows the parameters used in configuring the network for the experiment. Badly behaving nodes (selfish nodes) amounting to up to 50% were simulated in the network and were responsible for dropping packets. Results from the experiment used to evaluate the proposed model are based on summarized multiple runs, and negligible variation is noticed.

TABLE 1
SIMULATED NETWORK CONFIGURATIONS

Parameter	Value
Number of Nodes	50
Speed	10 m/s
Routing Protocol	AODV
MAC	802.11
Source-destination Pairs	15
Transmitting Capacity	2Kbps
Packet Size	512B
Simulation	500s
Trust Threshold	0.5
Number of Particles	50
Inertial Weight (w)	1.0
Cognitive Parameter (c1)	2.0
Social Parameter (c2)	2.0
Iteration Count	100

6.1 Performance Metrics

The performance of the entire simulated network is represented by five parameters:

1. Network throughput: the amount of digital data per time unit delivered over a physical or logical link. It is measured in bits per second (bits/s or bps), occasionally in data packets per second or data packets per timeslot
2. Packet loss: This is measured as the percentage of packets delivered successfully to the target nodes.
3. Energy consumption in the presence of misbehaving nodes.
4. The percentage of using trusted evaluated nodes above the trustworthiness threshold.
5. The effect of multi-dimensional social trust metrics and Quality of Service (QoS) metric.

7. RESULTS ANAYSIS

7.1 The Network Throughput Analysis

Upon simulating a MANET environment with configurations state in table 1, fig. 2 shows the performance of the throughput in the presence of misbehaving nodes. The y-axis shows the percentage of throughput for the standard PSO, and Proposed model (after evaluating trustworthiness using the proposed model), in the presence of misbehaving nodes. It is observed that the network throughput for the proposed system routing protocol outperforms the standard PSO.

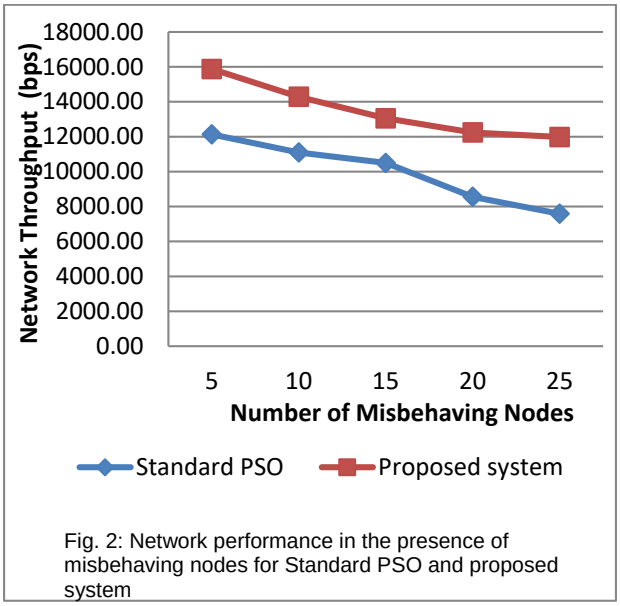

Fig. 2: Network performance in the presence of misbehaving nodes for Standard PSO and proposed system

At the presence of 5 misbehaving nodes the proposed system performs marginally better than the standard PSO in improving the overall network throughput by 23.57%. This trend is also evident as the number of misbehaving nodes increase in the network. However, presence of more malicious nodes affects over throughput of the network but the proposed system model still outperforms its counterpart by a slightly greater margin, improving network performance by 36.67%.

7.2 The Packet Loss Analysis

The impact of misbehaving nodes on packet loss is shown in Fig. 3. The percentage of packet loss rises with an increase in the percentage of misbehaving nodes, from nearly 10% when there are only 5 misbehaving nodes in the network, to less than 40% when the percentage of misbehaving nodes increases to half of the total population.

For the prop

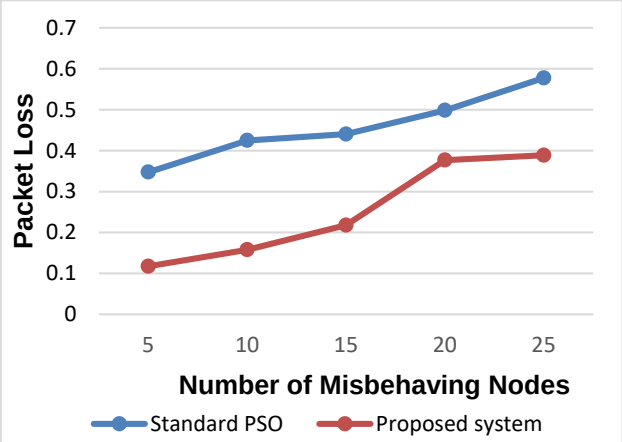

Fig. 3: Network packet loss in the presence of misbehaving nodes for standard PSO and proposed systemand proposed system

osed system, the packet loss percentage is significantly lower than standardized PSO model by 37.70%. It becomes evident from the above analysis that the social proposed system model performs better in terms of the packet loss metric by considering more social attributes of trust and QoS trust.

7.3 Energy Consumption

Fig. 4 shows the impact of misbehaving nodes on energy consumption. The energy consumed per byte is shown on the y-axis in the presence of misbehaving nodes. From the figure, it is obvious that the energy consumption percentage in the proposed system is less than Standard PSO routing protocol as it is able to reduce the number of dropped packets than both protocols. It is also observable that the energy level in the standard PSO is slightly different from the proposed protocol: especially when the percentage of misbehaving nodes is less than 30%.

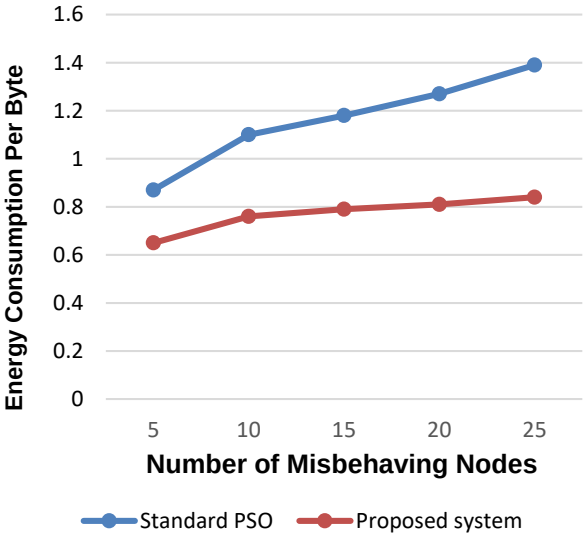

Fig. 4: Energy consumption in the presence of misbehaving nodes for standard PSO and Proposed system.

8. SYSTEM EVALUATION

8.1 Node Evaluation

The fig. 5 presents the evaluation of the proposed model in accurately evaluating trusted node in the network environment and choosing good nodes for communication path generation. It shows that the as the number of misbehaving nodes increase in a network environment the accuracy slightly reduces but at a very minute rate. When 5 malicious nodes existed in the network, the proposed system model was at an accuracy of 99.31%. Increasing the misbehaving nodes to 50, the accuracy level dropped slightly to 98.75%, representing a mere 0.56% difference.

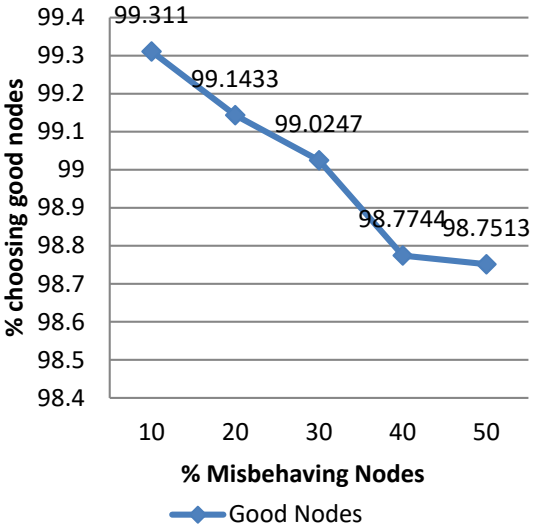

Fig. 5: Effective node evaluation in the presence of misbehaving nodes for standard PSO and proposed system.

8.2 Effect of Trust Metrics of the proposed system

This section presents the value of the social trust and QoS trust components used to produce the composite trust metric of the proposed system in relation to the number of interactions.

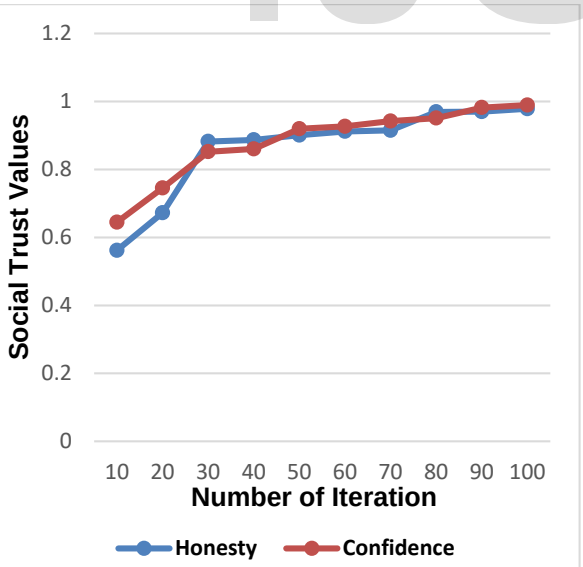

Fig. 6: Effect of social trust value metric of the proposed system with number of iteration.

Fig. 6 demonstrates the value of social components: honesty and confidence. It is seen that these values are changed by increasing the number of interactions. In contrast, Figure 7 shows that the estimated energy value of the evaluated node decreases as it becomes involved in more interactions with other nodes in the network. Consequently, the evaluation of the components used to calculate trust shows that the proposed model is able to effectively consider the dynamic characteristics of MANETs by using social and QoS trust.

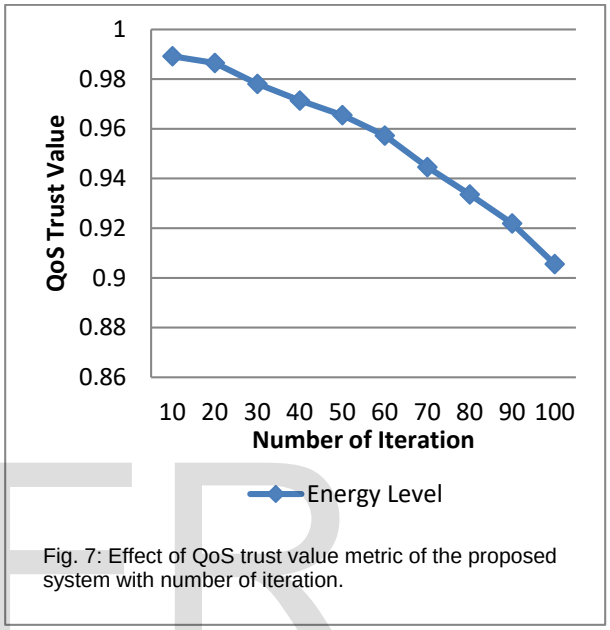

Fig. 7: Effect of QoS trust value metric of the proposed system with number of iteration.

9 SUMMARY AND CONCLUSION

The proposed system optimization model for trust management system to evaluate the trustworthiness of participating nodes in mobile ad-hoc networks was tested against benchmark functions to prove its correctness and quick convergence edge. The model was the incorporated into a simulated MANET environment using specially configured parameters and from the network analysis.

It therefore infers that the proposed model can keep the network performance metrics of throughput, packet loss, and energy consumption at a very high and acceptable level even when the percentage of misbehaving nodes is half of the total population in the environment consequently implies that trustworthiness of the proposed system is an improvement over the existing model.

From the analysis it showed that while the presence of malicious nodes affects the overall throughput, the

proposed system model marginally outshined the standard PSO counterpart by improving the network performance by 36.67%. Also, percentage packet loss in the network significantly reduced using the proposed system model designed using the proposed trust metric cost function by considering more social attributes of trust and QoS trust. Further, when evaluating the energy consumption of the proposed trusted model, it was shown from the experiment that the energy consumption percentage in the proposed system is less than Standard PSO routing protocol as it is able to reduce the number of dropped packets. Overall, it can be concluded that the proposed model can keep the network performance metrics of throughput, packet loss, and energy consumption at a very high and acceptable level even when the percentage of misbehaving nodes is half of the total population in a MANET environment.
MANET environments are characterised by constrained resources in terms of communication, memory usage and computational complexity requirements. Besides, such environments suffer from several points of failure which require techniques to enhance the decision making on nodes trustworthiness. This model balances trade-offs between energy consumption, accuracy of trustworthiness and network performance through a lightweight hybridized optimization technique, which represents important future direction of trust management in MANET.

This makes the model most suitable for distributed network environment that is prone to network attacks, where security and trust is highly regarded, and low energy consuming devices. It also allow the military take advantage of common place network technology to maintain a secure information network between the soldiers, vehicles, unmanned drones and military information headquarters, especially in hostile and remote environments.

10 FUTURE WORK

In this research work, a set of social and QoS properties of trust were used to model the behaviour of nodes in MANETs. These models can be extended by using more social and QoS properties to detect any malicious or bad behaving like newly joined nodes or changing identities. Dealing with such attacks is still an open and challenging problem of trust models. A comprehensive study of the effect of social and QoS trust on the trustworthiness evaluation process, and which properties have more importance on the nodes decision is also missing in the trust research. In addition, dynamic weightings and giving different importance to the different factors at different times of nodes' neighbourhoods is still an open problem needs to be considered in future.

REFERENCES

[1] Angeline, P.J. (1998). Evolutionary optimization versus particle swarm optimization: philosophy and performance difference, in: V.W. Porto et al. (Eds.), Proceedings of 7th Annual Conference on Evolutionary Programming, Lecture Notes in Computer Science, vol. 1447, Springer, Berlin, 1998, pp. 601–610.

[2] Bao, F., Chen I.R., Chang M., and Cho, J.H. (2011). Hierarchical trust management for wireless sensor networks and its application to trust-based routing. Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1732- 1738.

[3] Bao, F., Chen, R., Chang, M., and Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, Network and service Management, IEEE Transactions on, vol. 9, pp. 169-183.

[4] Beni, G., W.J. (1989). Swarm intelligence in cellular robotics systems: NATO Advanced Workshop on Robots and Biological System.

[5] Bin, Y., Zhong-Zhen, Y., and Baozhen, Y. (2009). An improved ant colony optimization for vehicle routing sensor networks, IEEE Communications Surveys & Tutorials, pp: 2-28.

[6] Dong, Y., Tang, J., Xu, B., and Wang D., (2005). An application of swarm optimization to nonlinear programming, Computers & Mathematics with Applications 49 (11–12) pp1655–1668.

[7] Dong, P., Wang H., and Zhang H. (2009). Probability-based trust management model for distributed e-commerce, Network Infrastructure and Digital Content. IC-NIDC. IEEE International Conference, pp. 419-423.

[8] Dorigo, M. (1992). Optimization, Learning and Natural Algorithms (in Italian). Ph.D. thesis, Dipartimento di Elettronica, Politecnico di Milano, Italy.

[9] Dorigo, M., Blum C. (2005). Ant colony optimization theory: a survey, Theoretical Computer Science 344 (2–3) (2005) 243–278

[10] Dorigo, M., Maniezzo, V., and Colorni, A. (1996). The ant system: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics - Part B 26(1):29–41

[11] Dorigo, M., Gambardella, L.M. (1997). Ant colony system: A cooperative learning approach to the travelling salesman problem. IEEE Transactions on Evolutionary Computation

[12] Dorigo, M., Di Caro, G. (1999). The ant colony optimization meta-heuristic, McGraw-Hill Ltd.,UK, Maidenhead, UK, England, pp 11–32 1:53–66

[13] Dorigo, M., Caro, G.D., Gambardella, L.M. (1999). Ant

algorithms for discrete optimization. Artificial Life 5(2):137–172

[14] Dorigo, M,. and Stützle, T. (2004). Ant Colony Optimization. MIT Press, Cambridge, ISBN: 978-0-262-04219-2.

[15] Goss, S., Aron, S., Deneubourg, J., and Pasteels, J. (1989). Self-Organized Shortcuts in the Argentine Ant, Naturwissenchaften, Vol. 76, pp. 579-581.

[16] Hao, Y., et al. (2004). Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE, 11(1): p. 38-47.

[17] Hazem, A., and Janice, G. (2012). Swarm Intelligence: Concepts, Models and Applications. Technical Report School of Computing Queen's University Ontario Canada.

[18] He, Q., Wu, D., and Khosla, (2004) P. "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks," Proc. IEEE Wireless Communications and Networking Conf., vol. 2, pp. 825- 830.

[19] Iftikhar, M.S., and Fraz, M.R. (2013). A Survey on Application of Swarm Intelligence in Network Security in Transactions on Machine Learning and Artificial Intelligence, Volume 1, No 1, PP 01-15.

[20] Karlson, P., and Lüscher, M. (1959). Pheromones: a new term for a class of biologically active substances. Nature, Vol. 183, pp. 55–56.

[21] Kavita, Prashant Sahai, and Sonu Mittal (2018) "Implementation and performance analysis of AODV-PSO with AODV-GA and AODV-ABC" International Journal of Engineering and Technology.

[22] Kennedy, J., and Eberhart, R.C. (1995). Particle swarm optimization. In Neural Networks, 1995. Proceedings. IEEE International Conference on. IEEE.

[23] Kennedy, J., and Eberhart, R.C (1995). Particle Swarm Optimization. In Proceedings of IEEE International Conference on Neural Networks, Perth, Australia, pp. 1942–1948.

[24] Kennedy, J., and Eberhart, R.C (1995). A new optimizer using particle swarm theory. In Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, pp. 39–43.

[25] Li, W., Parker, J., and Joshi A. (2012). Security through collaboration and trust in MANETs, Mobile Networks and Applications, vol. 17, pp. 342-352.

[26] Li, R., and Li, J. (2013). Requirements and design for neutral trust management framework in unstructured

[27] Lloyd, C. (2003). The alarm pheromones of social insects: A review, Technical report, Colorado State University.

[28] Luo, J., Liu, X., and Fan, M. (2009). A trust model based on fuzzy recommendation for mobile ad-hoc networks. Computer Networks, vol. 53, pp. 2396-2407.

[29] Nagalakshmi, S., and Rakesh, P. (2016). Performance Comparison and Evaluation of Efficient Routing Protocols for MANETs: Ant Inspired Adaptive Routing. International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 9.

[30] Nekkantim R.K., and Lee, C. (2004) "Trust-based Adaptive On Demand Ad Hoc Routing Protocol," Proc. 42th Annual ACM Southeast Regional Conf., Huntsville, Alabama, 2004, pp. 88-93.

[31] Ourique, C.O., Biscaia, E.C., and Pinto, J.C.(2002). The use of particle swarm optimization for dynamical analysis in chemical processes, Computers & Chemical Engineering 26 (12) 1783–1793.

[32] Paterlini, S., and Krink, T. (2006). Differential evolution and particle swarm optimisation in partitional clustering, Computational Statistics & Data Analysis" 50 (5) 1220–1247.

[33] Ramireddy Kondaiah and Bachala Sathyanarayana (2018) "Trust and Fuzzy- Ant Colony Optimization based Intrusion Detection System for Secure Routing of MANET" International Journal of Computer Science and Mobile Computing, Vol.7 Issue.4, April- 2018, pg. 59-75

[34] Reynolds, C.W. (1987). Flocks, herds, and schools: A distributed behavioural model, Computer Graphics (ACM SIGGRAPH '87 Conference Proceedings), Vol. 21, No. 4, pp. 25–34.

[35] Shabut, A.R.M. (2015). Trust Computational Models for Mobile Ad Hoc Networks, a Ph.D. thesis submitted to School of Computing Faculty of Engineering and Informatics University of Bradford

[36] Shabut, A., Dahal, K.P., and Awan, I. (2013). A Recommendation-Based Trust Model for MANETs to Enhance Dynamic Recommender Selection Using Multiple Rules, Seventh International Open Conference HET-NETs 2013, UK, Ilkely.

[37] Shabut, A., Dahal, K.P., Awan, I. (2013). A Trust-Based Monitoring Model to Secure Routing Protocol in MANETs Using Enhanced Trust Metric", Seventh International Open Conference HET-NETs 2013, UK, Ilkely, 2013.

[38] Shabut, A., and Dahal, K.P. (2011). Trust and Security Management in Distributed Systems, University of Bradford school of computing, School Research seminars.

[39] Sharvani G.S. (2012) "Development of Swarm Intelligent Systems for MANET" A Ph.D Thesis submitted to the Department of Computer Science and Engineering, Faculty of Engineering, Avinashilingam University for Women, Coimbatore

[40] Shelokar, P.S., Jayaraman, V.K., and Kulkarni, B.D. (2004). An ant colony classifier system: application to some process engineering problems. Computers & Chemical Engineering 28 (9) (2004) 1577–1584

[41] Shelokar, P., Siarry, P., Jayaraman, V. K., & Kulkarni, B. D. (2007). Particle swarm and ant colony algorithms hybridized for improved continuous optimization. Applied Mathematics and Computation, 188(1), 129–142.

[42] Shi, Y (2004) "Feature article on particle swarm optimization", IEEE Neural Network Society, Feature Article, pp. 8–13.

[43] Shyu, S.J., Yin, P.Y., Lin, B.M.T. (2004). An ant colony optimization algorithm for the minimum weight vertex cover problem. Annals of Operations Research 131:283–304

[44] Shyu, S.J., Lin, B.M.T., and Hsiao, T.S. (2006). Ant colony optimization for the cell assignment problem in PCS networks, Computers & Operations Research 33 (6) (2006) 1713–1740.

[45] Sumit Kumar, Madan Lal Saini, and Sandeep Kumar (2018) "A Survey: Swarm Based Routing Algorithm toward Improved Quality of Service in MANET" International Journal of Management, Technology And Engineering Volume 8, Issue V, ISSN NO : 2249-7455.

[46] Wang Y.D., and Emurian, H .H. (2005). An overview of online trust: Concepts, elements, and implications, Computers in human behavior, vol. 21, pp. 105-125, 2005.

[47] Wang, Y.F., Hori, Y., and Sakurai, K. (2008). Characterizing economic and social properties of trust and reputation systems in P2P environment, Journal of Computer Science and Technology, vol. 23, pp. 129-140, 2008.

[48] Wang, Y. and Vassileva, J. (2003). Trust and reputation model in peer-to-peer networks. Peer-to-Peer Computing, 2003. (P2P 2003). Proceedings. Third International Conference on, 2003, pp. 150-157

[49] Yin, P.Y., and Wang, J.Y., (2006). Ant colony optimization for the nonlinear resource allocation problem. Applied Mathematics & Computation 174 (2)

[50] Yunfang, F (2007) "Adaptive Trust Management in MANETs," Proc. 2007 Int'l Conf. on Computational Intelligence and Security, Harbin, China, pp 804-808.