International Journal on Emerging Technologies **11**(2): 104-109(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Secured Ant Colony Optimization based on Energy Trust System for Replica Node Attack Detection

S. Anitha[1], P. Jayanthi[2], K. Lalitha[3] and V. Chandrasekaran[4]
[1]Assistant Professor, Department of Information Technology,
Kongu Engineering College (Tamilnadu), India.
[2]Associate Professor, Department of Computer Science and Engineering,
Kongu Engineering College (Tamilnadu), India.
[3]Assistant Professor, Department of Information Technology,
Kongu Engineering College, (Tamilnadu), India.
[4]Professor & Head, Department of Medical Electronics,
Velalar College of Engineering and Technology (Tamilnadu), India.

(Corresponding author: S. Anitha)
(Received 28 November 2019, Revised 18 January 2020, Accepted 23 January 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Construction of cloud computing and promotion of applications such as social network service and smart city have driven the need for trust mechanism with the rapid developments of Internet of things (IoT). In the existing methods, storing the trust value incurs high storage overhead leading to energy inefficiency and reliability of identifying trustful or untrustworthy node is very less. In order to avoid these drawbacks, Secured Ant Colony Optimization (SACOP) based on trust sensing model is proposed to detect the node replication attack. Firstly, node's trust value is estimated using direct and indirect trust evaluation model to identify the malicious node in the clustered network. Secondly, ant colony routing algorithm is introduced to select the secured optimal path using probability to select the next hop node for data forwarding. As the probability is calculated using the residual energy, trust and pheromone values, energy expenditure among all nodes gets balanced. The proposed algorithm performs better in terms of packet loss rate, time delay, throughput and average energy consumption compared to existing scheme DDR.

Keywords: Ant colony Optimization, Pheromone, Probability**,** Replication attack, Trust.

Abbreviations: IoT, Internet of Things; WSN, Wireless Sensor Networks; SACOP, Secured Ant Colony Optimization; CM, Cluster Member; CH, Cluster Head; BS, Base Station; ID, Identity.

I. INTRODUCTION

In aspects of diagnosis, monitoring and surveillance, smart city offers wide applications for urban residents. Physical information around the environment is collected using ubiquitous sensor nodes [1]. Sensor nodes make use of distributed facilities to operate in unattended environment. Although WSNs is an open and distributed system, it is vulnerable to attacks due to its simplicity and resource-restraint in the design of hardware unit [2]. Moreover, the attack is more probable because of the wireless communication channel. The conventional protocol design available in the existing work is inappropriate due to its complexity for resource-limited WSNs [3]. The security aspects such as authentication, encryption, verification of information integrity and intrusion detection are widely applied in many researches in wireless sensor network.

There are many attacks that penetrate inside the network and destroy the normal operation of the node while most of the security mechanisms deal with attacks from the perimeter of the network [4]. Selfish node, malicious forwarding, black hole, rushing or worm attacks are few examples of insider attacks [5, 6]. A popular and effective method is the trust model-based management mechanism [7]. In respect of solving internal attacks and identifying malicious nodes trust evaluation model demonstrates a significant advantage since it involves low computation and communication load [8]. Most of the existing work concentrates on either energy utilization or attack node detection. Only few papers deals with the optimized result of both energy efficiency and attack node detection. But that too have more false alarm rate in detecting attack nodes. So the objective of the proposed work is to reduce false alarm rate with reduced energy consumption. An attack in which many replica nodes are created from a single original node in the network is known as replica node attack. Nodes are captured and re-programmed by the adversary and the region which holds such nodes is known as replica node region. The contributions made in this paper are:

– reduced packet loss rate
– reduced time delay
– improved throughput
– reduced average energy consumption

The rest of the sections in this paper are organized as follows: Section II discusses the existing work. System design and various phases of the proposed method are described in Section III. In Section IV, the simulation results are given with the performance evaluation. Finally, conclusion is given in Section V.

II. RELATED WORK

Credible trust management scheme is proposed based on Bayesian theory for WSNs [9]. Initially, RFSN model is used to find trust value estimate and comprehensive

trust value is acquired using statistical data and Bayesian method. The trust value's restoration is done using time sliding window if third parties involved in evaluation of trust value.

For selectively evaluating the direct and recommended trust values, distributed trust evaluation model for WSNs is proposed [10].

Distributed trust management system with fuzzy theory is proposed to measure the trust value of nodes in WSNs [11].

Trust evaluation model is used to identify malicious nodes or selfish nodes effectively for intrusion detection. Then the trusted routing path is created by eliminating malicious nodes [12].

Social and QoS (quality of service) trust values are formulated for evaluating trust based on intimacy or honesty metrics in Hierarchical trust management protocol [13]. Based on energy dissipation and node selfishness, it selects QoS' trust.

The mechanism for detecting dishonest recommendation in indirect trust computation is proposed [14]. Based on the dissimilarity value from the complete recommendation set, this method detects dishonest recommendations. A dissimilarity function is evaluated to capture the dissimilarity of recommendation class from the median of the recommendation set, since median is resistant to outlier.

For quantized target tracking in WSNs, secure and robust clustering is proposed [15]. Based on adaptive QVF algorithms, the problem of secure clustering for target tracking in wireless sensor networks is performed.

There are enormous routing and attack detection strategies and its applications in WSNs are studied [16, 17].

The existing system has drawbacks as, trust value is calculated for a node based on the recommendations from all of the neighbours and storing the trust value as float instead of integer incurs high storage overhead, it is not efficient in terms of energy. Though recommendations are received from all its neighbor nodes for any node, the reliability of identifying trust or untrust node is very less as it does not take into account nodes' behavior in terms of attacker model and only combining subjective judgment and objective evaluation.

A. Identification Of Research Gap

The solutions to replica node detection should follow design goals as follows:

- Detection procedure can be made more robust and difficult to break it by the attacker. Specifically, the replica nodes must be detected before the attacker compromises substantial number of nodes
- Detection procedure can be improved to have high detection accuracy in detecting only compromised nodes as replicas. If so, then it can be used as a preventive tool to detect other DoS attacks

III. SECURED ANT COLONY OPTIMIZATION (SACOP)

Direct and indirect trust calculation is done to identify the trustful or untrustworthy nodes correctly. Based on the residual energy of nodes, next hop node is selected for forwarding the data. Other factor such as trust can also be involved in selecting the optimal path.

A. System Design

The overall design of SACOP is shown in Fig. 1.

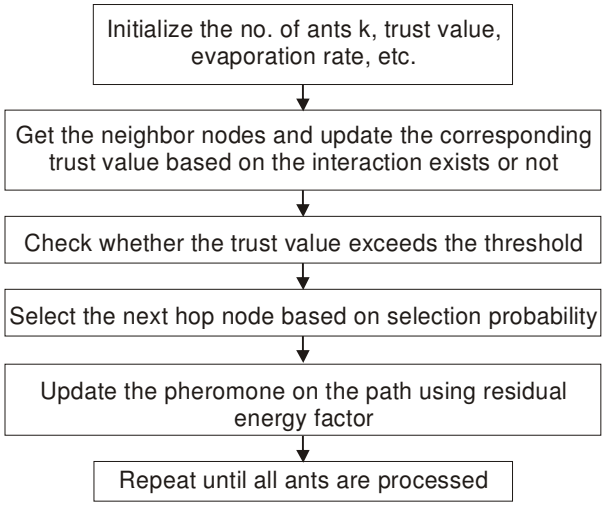

Fig. 1. Overall design of SACOP.

B. Proposed Algorithm

In order to provide a solution to overcome internal attacks, the proposed SACOP algorithm uses trust evaluation model to isolate replica nodes effectively. STEOAP is used to find the optimal path for detecting the replica node based on the selection probability. The probability for selecting the next hop node in the path is calculated based on three factors, pheromone factor, heuristic value and residual energy factor. Earlier works mostly depend on node's residual energy in selecting the optimal path. So, energy expenditure among all nodes should be effectively balanced in clustered network, thereby improving the lifetime of the network. In the proposed method, optimal path also includes trust value for detecting replica node by comparing with the threshold of trust value. The proposed method consists of following stages

C. Node deployment and localization

The first phase of SACOP algorithm is the deployment of the nodes at random position (uniform distribution) and updating the location information to the sink node. Nodes ranging from 100 to 350 are deployed uniformly over the given area and it is stored in the database. The nodes can be accessed by its index value. The sink node floods the broadcast message which contains fields such as s_id, seq_no., s_x, s_y and visited-node_list where s_id is the sensor node identity, seq_no. is the sequence number of the message, s_x and s_y are the x and y position of sensor nodes, visited-node_list is initially empty and index value is stored in the list while each sensor node updates its location.

When the index is not present in the list, index value is updated as the identity of the node and location as the address of the node. Otherwise, the message is deleted. The broadcast identity is taken as the sequence number of the message. The sensor nodes updating their location information to the sink is given as Fig. 2.

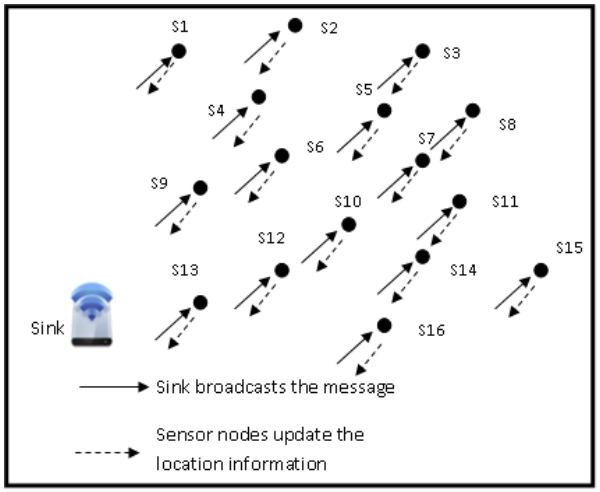

Fig. 2. Upon location information request as a broadcast message from the sink node, sensor nodes update their location in the reply message.

By visiting all the non-visited nodes, node id, sequence number, location are updated in the sink node.

D. Cluster formation and cluster head election

The clustering process starts with the collection of information from all the sensor nodes. After collecting the information, the sink initiates the clustering process in a centralized manner. Thereafter, cluster maintenance as re-election of CH is carried out by all sensor nodes in a distributed manner. The updates of cluster maintenance are periodically pulled by the sink in order to maintain better connectivity with the sensor nodes.

The sink node first chooses the cluster head having higher probability after knowing the location information of sensor nodes. The node's probability of becoming a CH is calculated by the sink node from the node's information and stored in the node's probability table. During the deployment phase, the node with greater probability is considered as the CH from the table which is sorted in descending order. The information of the newly formed CH is broadcasted to all the nodes and the CH starts receiving the data. For instance, network containing 16 nodes with node's probability to become a cluster head is listed in decreasing order is shown as Table 1.

Table 1: Probability values of nodes in descending order.

Node_ID	13	15	12	7	1	2	3	4	10	5	8	9	11	16	14	6
Probability	0.9	0.86	0.75	0.78	0.65	0.64	0.55	0.51	0.45	0.40	0.35	0.32	0.25	0.23	0.15	0.11

The first node which has highest probability value is selected as the cluster head with its entire one-hop neighbors as its cluster members. So, if node 13 is chosen as the cluster head, its one-hop neighbors, 6, 9, 10 and 12 are grouped under cluster head 13 as its cluster members. Then these nodes are removed from the probability table and procedure is repeated until all the nodes are attached under any of the cluster.

Two lists namely, cluster head list and cluster member list are maintained by the sink node. Each node is removed from the table and is added in the corresponding list. The node status is indicated based on the nodes presence in cluster head list or cluster member list. This is shown for the total number of 16 nodes in Fig. 3.

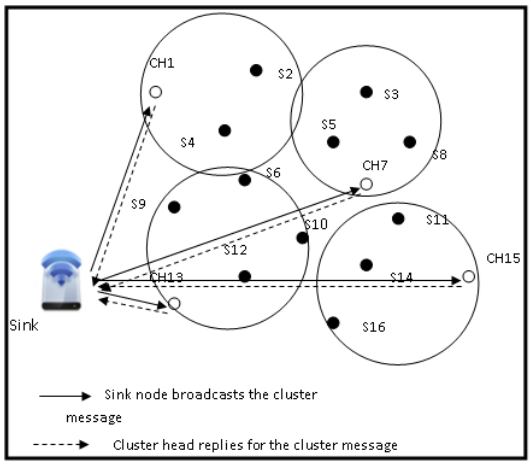

Fig. 3. Clusters are formed after selecting the cluster head and cluster members from the sorted residual energy values of nodes stored in the probability table.

Based on the clustering parameters such as energy, node connectivity, bandwidth and traffic pattern of the node, cluster group can maintain better hop connectivity.

E. Cluster updating process

If any CH node is on the threshold of completely being drained of energy level, it broadcasts a message denoting its expiry to both its cluster members and predecessor CHs in the forward path. On receiving the expire message from the CH, the member nodes estimate the probability to elect a new CH. The elected node acts as the CH and sends a message to the sink. The sink updates its tables during the next iteration. The proposed work in which CH selection is initiated by the sink in a centralized manner and thereafter the individual clusters select their CH in the event of failure of their current CH. Hence this approach uses both centralized and distributed mechanism of CH selection.

F. Trust calculation

Two types of trust values are calculated viz., Direct and indirect trust values. After checking the ID and position of the nodes stored in CH and BS for CMs and CHs respectively, residual energy of the nodes are calculated using the expression,

$$E \geq \sum(E_{total} + \lambda 1) \quad (1)$$

If the condition specified in Eqn. (1) is satisfied, successful interaction count is incremented.

$$s = s + 1$$

Otherwise, unsuccessful interaction count is incremented.

$$u = u + 1$$

Direct trust value: Based on the number of direct interaction between node *i* for node *j*, direct trust value is calculated. The behavior of neighbor nodes is monitored during interactive communication and by

using the node's trust value. If interaction exists, direct trust value between the nodes is measured using mean value as shown in Eqn. (2),

$$T_{dir}(i,j) = \frac{\propto_{ij}+1}{\propto_{ij}+\beta_{ij}+2} \quad (2)$$

where $\propto_{ij}$ and β_{ij} are the number of successful and unsuccessful interaction between nodes *i* and *j*. To avoid number of failed interactions due to network congestion and noise, penalty function δ is used to compensate the trust value.

$$\delta = 1 - e^{\frac{\beta_{ij}}{\propto_{ij}+\beta_{ij}}}$$

To avoid number of successful interactions due to abnormal behavior of malicious node satisfying the threshold regulator function μ is used.

$$\mu = 1 - \frac{1}{ln\left(\propto_{ij}+1\right)}$$

Combining above two functions, direct trust value can be calculated as shown in Eqn. (3),

$$T_{dir}(i,j) = \frac{\mu\propto_{ij}+1}{\mu\propto_{ij}+\beta_{ij}+2}\delta \quad (3)$$

Indirect trust value: When interaction does not occur with any node, indirect trust value of the node is calculated. The behavior of the node with its common neighbours between the interacting nodes is considered for indirect trust value. Compared to the direct trust value, indirect trust value gives the right evaluation for a node based on the threshold. This is illustrated in Eqn. (4).

$$T_{ind}(i,j) = \frac{\sum_{m\in Ns, m\neq i} T_{dir}(i,m)\times T_{dir}(m,j)}{|N(i)\cap N(j)|} \quad (4)$$

Based on the communication behavior of the nodes, weightage is assigned. The summation of the direct and indirect trust value weightage is considered as the comprehensive trust value which gives the reliability for differentiating between normal and replica node. This is shown in Eqn. (5)

$$T_{total}(i,j) = \theta T_{dir} + (1-\theta)T_{ind} \quad (5)$$

If the node ID and position is illegal that is, the ID and position value stored has duplication or does not exists, the received message is deleted. It is assumed that the message is originated from a replica node.

G. Forward Tree Establishment and Data Transmission

In order to select the optimal path, next hop neighbor is selected according to pheromone concentration which depends on nodes residual energy and evaluated trust value. Each ant moves from source node to destination node through intermediate nodes. The intermediate nodes are selected as the next hop node based on the higher selection probability.

$$p_{ij}^{k}(t) = \left\{ \begin{array}{c} \frac{[\tau_{ij}(t)]^{\alpha}.[n_{ij}(t)]^{\beta}.[\varphi_j(t)]^{\gamma}}{\sum_{u\epsilon Nk(i)}[\tau_{iu}(t)]^{\alpha}.[n_{iu}(t)]^{\beta}.[\varphi_u(t)]^{\gamma}}, j \in N(i) \\ 0, otherwise \end{array} \right\}$$

The forwarder node forwards the sensed data to the next successor node and this is repeated until data reaches the sink thereby completing the data transmission and collection processes. The forward path is established by transmission of Sink_discmsg to the sink and updates the cluster group based on cluster member list and cluster head list. If the node is already visited or the sequence number of the packet is older, then the packet is not forwarded and is dropped, otherwise, the packet is forwarded to the node selected based on the probability value calculated. This is repeated until the packet reaches the sink node.

During data forwarding, energy-efficiency is considered as the important aspect. The transition energy should reflect the superiority of the node. $\varphi_j(t)$ denote the residual energy factor which is defined in Eqn. (6) as,

$$\varphi_j(t) = |N(i)| * E_{res}(j)/\sum_{s\in N(i)}\left(E_{res}(s)\right) \quad (6)$$

The next hop node is chosen from the neighbor nodes which is having highest comprehensive trust value. Then the heuristic factor $n_{ij}(t)$ is given in Eqn. (7),

$$n_{ij}(t) = argmax_{j\in N(i)}\{\theta T_{dir} + (1-\theta)T_{ind}\} \quad (7)$$

The increment of the pheromone is obtained using the Eqn. (8),

$$\Delta\tau_k(t) = \frac{E_{res}^{(t)}(i)/avg_{s\in N(i)}\left(E_{res}(s)\right)}{E_0 - max_{s\in N(i)\{(E_{res}(s))\}}} \quad (8)$$

where $N(i)$ be the neighbor of i,E_0be the initial energy and $avg_{s\in N(i)}\left(E_{res}(s)\right)$ be the average residual energy and $max_{s\in N(i)\{(E_{res}(s))\}}$ be the maximum residual energy.

The pheromone factor on the path is updated by using the Equation (9),

$$\tau_{ij}(t) = (1-\rho)\tau_{ij}(t) + \Delta\tau_k(t) \quad (9)$$

ρ represents the volatilization coefficient of pheromone.

If interaction exists between node i and j,

$$n_{ij}(t) = T_{dir}(i,j)$$

If interaction does not exists between node i and j,

$$n_{ij}(t) = T_{ind}(i,j)$$

Repeat the above steps for next ant, $k = k+1$

H. Detection of replica attack and route maintenance

Replica node is the node whose trust value is less than the threshold. The trusted node is the node having trust value greater than the threshold. The trust value of the attack node is calculated by the recommendation provided by its neighbors. Then that node is removed from the network.

Algorithm:

Begin

Initialize trust T, threshold λ, pheromone $\Delta\tau_k(t)$and energy $\varphi_j(t)$

While stopping criterion not satisfied do

Position each ant k in a starting node

Repeat

do

For each node x do

Calculate the direct $T_{dir}(i,j)$ and indirect $T_{ind}(i,j)$ trust values

If $(T^x{}_{total}(i,j) > \lambda)$

Choose next node by applying selection probability $p_{ij}^{k}(t)$

Apply step by step pheromone update $\tau_{ij}(t)$

else

Remove the node from the path

End for

Until every ant has built a solution

Update best solution

Apply offline pheromone update

End while

End

IV. RESULTS AND DISCUSSION

The simulation experiments are conducted for SACOP using NS-2 for performance evaluation. SACOP algorithm shows improved results compared to DDR in

terms of performance metrics such as packet loss rate, end-to-end delay, throughput and average energy consumption. The simulation parameters are shown in Table 2.

Table 2: Experimental parameters.

Parameters	Values
initial energy, E_0	0.7 J
Initial value of trust	0.8
Length of the packet	2000 bits
d_0	37 m
E_{elec}	50 nJ / bit
E_{da}	5 nJ / (bit signal)
Trust Theshold, λ	0.9
Weight of direct trust, Θ	0.9
Link layer protocol	MAC 802.11
Type of queue	PriQueue
Flow rate of data	448 kbit/s
weight value of pheromone, α	0.5
weight value of heuristic value, β	0.2
weight value of residual energy factor, γ	0.3
Volatilization coefficient of pheromone, ρ	0.3

The number of interactions is reduced due to increase in packet loss rate, when the number of replica nodes is increased. So, energy consumption decreases after certain point as it also depends on the number of interactions count. As the number of nodes increases, it balances with the increasing replica nodes and average energy consumption remains stable. Also, pheromone value is updated based on the residual energy of the node which is one of the factors in selection probability calculation. Average energy expenditure is balanced among all sensor nodes in the network. This is shown in Fig. 4.

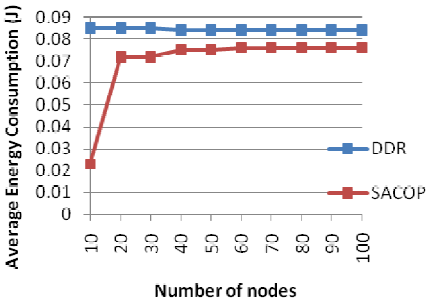

Fig. 4. Average Energy Consumption.

As SACOP and DDR make use of the trust model to assess the behavior of the node, packet loss is comparatively lower. But in replica attack, data packets forwarding is affected with increase in packet loss as shown in Fig. 5. When the number of nodes increases, SACOP increases the speed of path search updating the pheromone, reduces the time delay, thereby reducing and stabilizing the packet loss rate due to clustering.

Due to massive data packets loss, reduction in throughput occurs. But due to the trust evaluation model used in SACOP and DDR, reduction in throughput is avoided. Hence, stability of the network is guaranteed. The overall throughput result shown in Fig. 6 demonstrates improved performance over DDR since the packet loss rate of SACOP is lesser.

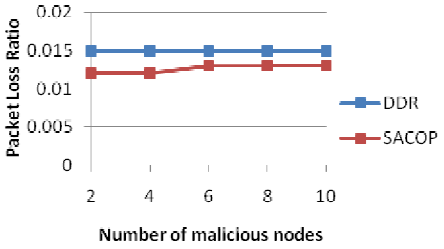

Fig. 5. Packet Loss Rate.

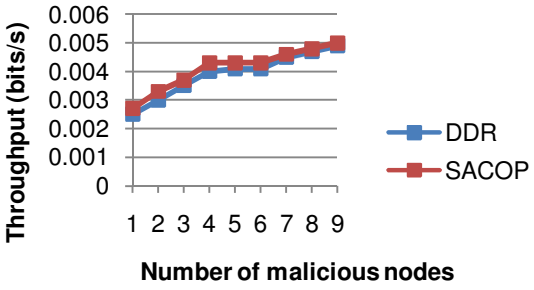

Fig. 6. Throughput.

Due to the excessive packet loss, routing stability drops when the number of replica nodes increases. Thereby the delay of packets arriving at the destination gets increased as shown in Fig. 7. As both SACOP and DDR uses the trust evaluation model, the trend in time delay is similar. In contrast to DDR, optimal path in SACOP is found based on the selection probability in which residual energy plays a main role by lowering the delay.

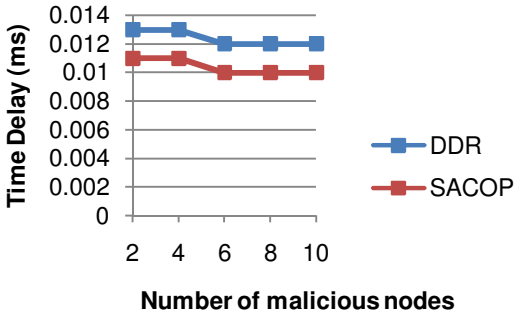

Fig. 7. Time Delay.

Fig. 8 illustrates the comparison of total trust value in the case of no attack and in the presence of attack for the existing DDR and proposed SACOP algorithms. As the number of successful interactions between nodes increases rapidly over time, total trust value of the node is also increasing in the case of no attack scenario. This steady increase is stabilized using the regulator function over a period of time. Thus the slow growth of trust value reflects the normal behaviour of nodes operating in the real-time environment which consists of congestion and noise.

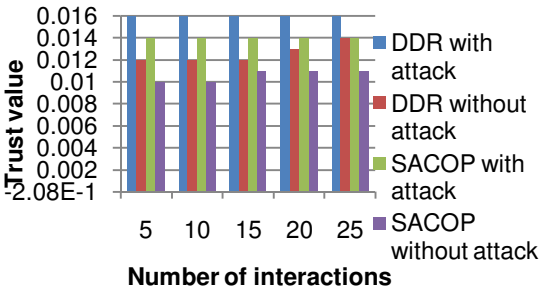

Fig. 8. Trust value.

As the number of unsuccessful interactions between the nodes continues to increase in the presence of attack, the trust value between nodes is reduced at a faster rate. In the proposed SACOP algorithm, the trust value is lesser than the trust value of DDR in all cases. This clearly indicates that SACOP algorithm is highly sensitive to attack characteristics compared to DDR. As a result, SACOP detects replica nodes accurately and quickly.

V. CONCLUSION

SACOP, a trust mechanism for detecting replica attack in clustered WSNs is proposed. A reliable evaluation model of trust perception using direct and indirect trust values is presented. It estimates nodes' behavior in terms of coverage range, signal strength, past successful and unsuccessful interaction counts and identifies replica nodes effectively. In the ant colony routing algorithm, trust evaluation model is introduced to improve the security of data forwarding. By obtaining the residual energy, pheromone is calculated. If the trust value is less than the threshold, then the node is considered as attack node and it is eliminated, otherwise, the node is considered as normal node. The results of the presented performance evaluation show that SACOP effectively detect replica attack in WSNs. Moreover, an analysis of the proposed SACOP approach indicates that the proposed system is highly secured compared with other trust mechanisms.

VI. FUTURE SCOPE

As most of the real-time environments involve mobility, extending trust calculation for mobile nodes will be concentrated.

Conflict of Interest. There is no conflict of interest.

REFERENCES

[1]. Eslaminejad, M. R., Sookhak, M., Razak, S. A., & Haghparast, M. (2011). A review of routing mechanisms in wireless sensor networks. *International Journal of Computer Scientific Telecommunication, 10*(2), 1–9.

[2]. Kellner, A., Alfandi, O., & Hogrefe, D. A., (2012). Survey on measures for secure routing in wireless sensor networks. *International Journal of Sensor Networking Data Communicatio, 1*(10), 1–17.

[3]. Chakrabarti, A., Parekh, V., & Ruia, A., (2012). A trust based routing scheme for wireless sensor networks. *Lecture Notes Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 1*(84), 159–168.

[4]. Duan, J., Yang, D., & Zhu, H. (2014). TSRF: a trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Network,* (1), 1–14.

[5]. Ishmanov, F., Malik, A. S., & Kim, S. W. (2015). Trust management system in wireless sensor networks: design considerations and research challenges. *Transaction of Emerging Telecommunication Technology, 26*(2), 107–130.

[6]. Lin, F., Xiahou, J. B., & Xu Z. X. (2016). TCM clinic records data mining approaches based on weighted-LDA and multi-relationship LDA model. *Multimedia Tools and Applications, 75*(22), 14203–14232.

[7]. Wei, W. and Yong, Q., (2011). Information potential fields navigation in wireless ad-hoc sensor networks. *Sensors 11*(5), 4794–4807.

[8]. Marchangl, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. *IET Information Security, 6*(2), 77–83.

[9]. Feng, R., Han, X., & Liu, Q., (2015). A credible Bayesian-based trust management scheme for wireless sensor networks. *International Journal of Distributed Sensor Networks,* (2), 1–9.

[10]. Jiang, J., Han, G., & Wang, F. (2015). An efficient distributed trust model for wireless sensor networks. *IEEE Transactions on Parallel and Distributed System, 26*(5), 1228–1237.

[11]. Hossein, J., & Mohammad, R. A. (2015). A fuzzy fully distributed trust management system in wireless sensor networks. *International Journal of Electronics and Communication, 9*(17), 1–10.

[12]. Dhakne, A. R., & Chatur, P. N. (2016). TCNPR: trust calculation based on nodes properties and recommendations for intrusion detection in wireless sensor network. *International Journal of Computer Science and Network Security, 16*(12), 1–10.

[13]. Bao, F., Chen, I. R. and Chang, M. J., (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transaction on Network Server and Management, 9*(2): 169–183.

[14]. Iltaf, N., Ghafoor, A., & Zia, U. (2013). A mechanism for detecting dishonest recommendation in indirect trust computation. *EURASIP Journal of Wireless Communication and Networking,* (1), 1–13.

[15]. Majdi, M., Lyes, K., & Hazem, N. (2013). Secure and robust clustering for quantized target tracking in wireless sensor networks. *Journal of Communication and Networking, 15*(2), 164–172.

[16]. Priyanka R., & Satyanarayan Reddy, K., (2020). A Comprehensive Survey on Energy Efficient Routing Techniques and Various Attacks in Wireless Sensor Networks. *International Journal on Emerging Technologies, 11*(2), 57-65.

[17]. Kiran I., Prasad N., Advait P., Krushna A., Ritikesh N., & KedarTonge (2019). Disaster Management using Wireless Sensor Network. *International Journal of Electrical, Electronics & Computer Science Engineering, 6*(2), 13-15.

How to cite this article: Anitha, S., Jayanthi, P., Lalitha, K. and Chandrasekaran, V. (2020). Secured Ant Colony Optimization based on Energy Trust System for Replica Node Attack Detection. *International Journal on Emerging Technologies*, *11*(2): 104–109.