ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

Secured Communication and Trust Based Protocol Model Using Whale Swarm Secure Clustering Algorithm

[1]Syed Mohd Ali, [2] Syed Abdul Sattar, [3] D. Srinivasa Rao
[1] Research Scholar JNTUH,[2] Principal NSAKCET , [3] Professor ECE Department JNTUH

Abstract: **- Heterogeneous Wireless Sensor Network users are increasing quickly in virtually every field of the infrastructure that needs for use efficiently. In WSNs, clustering is a useful technique to expand that network's lifetime and to protect each node in wireless networks. With several secure and reliable optimizations, or secure local optimization, many real-world optimization issues arise. Because of the untrustworthy architecture in a local and global environment, these nodes face communication skills issues such as small range and high throughput, which are likely to limit wireless communications in WSNs, making it difficult for WSNs to function properly. Another issue is the security and privacy factor where multiple sensors are unable to prevent unauthorized access and malicious attacks which lead to breaches of security. To address communication capacity issues and stable sensor systems (SS), we proposed a new framework called the Secured Communication and Trust-based Protocol Model (SC-TBPM) that takes into account reliability, protection and responsiveness. This model uses a Whale Swarm secured clustering Algorithm (WSSC) that mainly focuses on trustworthy nodes as cluster heads (CHs) by considering security parameters such as residual energy (ER), node density (DN), and average cluster distance (ADC).**

Keyword:- Whale swarm secure clustering Algorithm, Trust based metrics, secure protocol model.

INTRODUCTION

Wireless Sensor Networks have been a most magnificent research field in the last few years [1]. A Wireless Sensor Network (WSN) comprises a large number of wireless sensor nodes, which form a signaling events and a drain. Such an immense number of cluster members would be able to see everything over their worlds, which execute small simulations and wirelessly touch the WSNs. Related parameters are performed such as sensors to detect like amount of nearest neighbors[2].

Node connectivity frequency evaluation, improvement, load balancing, etc. Cooperation between those nodes can be achieved. Such functions produce wireless sensors which are very useful in monitoring phenomena of normal load-energy parameters, improving performance, predicting coverage of flow ranges. Such tasks include the highly realistic sensor networks. There is growing interest in research into heterogeneous wireless sensor networks to establish additional-reliable sensing devices [3].

Protection is one other critical problem which has arisen as consequences of these WSNs re- chargeable existence. Based on few similarity measures like distance (D), contact range (CR) etc. [4] these classes are formed by combining WSNs. This method is called clustering for grouping the nodes into classes. Clustering aims to improve network scalability and robustness. WSNs have two fundamental obligations: (i) sensing environmental conditions and (ii) transmitting the valuable knowledge towards the outside world. Compared to the sensing element conducted by such entities, data communication between these nodes affects similarly and contributes to too many security concerns. [4] Therefore, due to the higher-energy dissipation, certain appropriate framework for optimal dissipation of energy from SN is very much needed to secure and protect the WSNs. Factors such as safety and security also play a major role in ensuring accurate and efficient data transmission at base station (BS) node. Unfortunately, WSNs are vulnerable to different kinds of internal as well as external security threats [5].

When communication occurs from several sensor networks and outside the system leading to many security problems in WSNs. Secured Clustering is one of the most effective techniques for safe and efficient data transfer in WSNs, retaining this security issue, to secure wireless sensor networks (WSNs), we have introduced a new model called secured whale swarm optimization model. In this model we will concentrate on the communication parameters such as how much quality and energy consumption between the

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

sensor nodes, contact between the neighboring nodes, nodes near the base station, node coverage area [6]. Concentrating on all of these variables while using a whale swarm optimization algorithm allowing cluster members to select the energy-conscious metrics that depend on even a given function that estimates the node's remaining power and the neighboring node's energy number. Hence secured clustering is very efficient technique for the secured and efficient communication in WSNs, keeping this security concern, to secure the wireless sensor networks (WSNs), we proposed a novel model called Secured Communication and Trust based protocol Model (SC-TBPM). In this model we will be focusing on the Security parameters like energy remaining(ER), density of node (DN), and average distance of cluster (ADC) by using a Whale swarm secured Algorithm (WSSA) mainly focuses on trust worthy nodes as cluster heads (CHs).

The papers are outlined into sections below. Section I addresses the introduction of WSNs. Section II Related work Section III is the conceptual scheme under which our methodology was structured into three components. One is network model, next is security model then whale swarm secured algorithm (WSSC) for SC-TBPM model. Section IV deals with the mathematical representation of SC-TBPM model. Section V is the simulation Results.

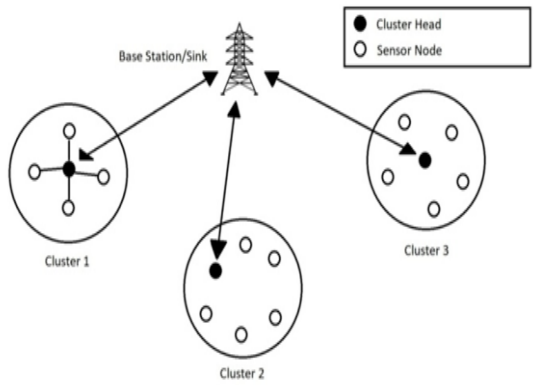

Fig. 1 Hierarchical Architecture of Cluster

RELATED WORK

Grid-based protocols, such as with the EEBCDA (Energy Efficient and Balanced Cluster-based Data Aggregation Algorithm) [7] and the EEBCDA multi-hop [8] will solve the hotspot problem effectively. Multihop EEBCDA is an EEBCDA-based enhancement. This splits the area of the network into several rectangles where each rectangle has an unequal number of grids, and the nodes form a cluster in each row. This method greatly decreases the amount of energy utilization and rises the lifetime of the network. Although the number of grids per rectangle is incoherent, excessive forwarding between all the layers is taking place. There is a situation where the upper layer nodes expired and data cannot be transmitted by the lower layer nodes that means a lot of energy waste [9].

EEMRP [10] suggested a grid clustering algorithm for clustering and proposed communication management (CM) nodes to distribute multi-hop data transmission. This technique efficiently tries to maintain the network's energy consumption, because the CM nodes share the CH nodes ' workload.

Swarm intelligence does have an important concept of self-association and self-organization which can offers a best solution for optimizing WSN routing protocols. Ari et al. [11] evolved a protocol for cluster-based power efficient routing called ABC-SD. This protocol uses artificial bee colony (ABC) search features which are used to design the cluster with low power consumption. The algorithm, however, utilizes a distributed technique for cluster head elections, and fixing the threshold energy is utilized to select CHs. When all of the cluster's energy is under the energy threshold, CHs may not be chosen.

Yalçın et al. [12] Suggested two algorithms based on bacterial interaction, namely CH selection, and a cognitive routing algorithm for the energy and transmission boundaries. Out of the result of simulation obtained from the program Mat lab 2016b (Math Works, Natick, USA), It would seem that the analysis is more robust in actual WSN situations, and appropriate.

Karaboga et al. [13] has suggested a clustering routing protocol focused on an artificial bee colony algorithm to maximize the lifespan of the network. The algorithm uses a QoS (Quality of Service) system to reduce the lags between the clusters receiving signals. This protocol did not, however, recognize the distribution of the CHs, those results in uneven energy consumption

Rao et al. [14] suggested an Energy Efficient Cluster Head Selection Algorithm (PSO-ECHS) depending on Particle Swarm Optimization that takes into account several parameters like intra cluster distance, sink distance and residual energy of sensor nodes to choose CH nodes. Some nodes far from CH nodes die early once the CH node chosen by the nodes has more residual energy but is far away from such nodes, due to various factors getting considered at the same time.

Kuila et al. [15] Have Used a PSO-based clustering algorithm to improve WSN life period. In this technique, the clustering is depends up on the average cluster distance and the gateway's life. The fitness value of every particle in the swarm is computed by using fitness function and this fitness value is used to judge the quality of the network. A particle

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

with better fitness function value gives better network structure.

Xiang et al. [16] suggested an Efficient Routing Algorithm depends on PSO capacity. The algorithm's fitness function considers node residual energy and transmission distance to some degree balancing the network's energy consumption.

Wang et al. [17] proposed an unique clustering method named Energy Centers searching for heterogeneous WSNs by using Particle Swarm Optimization (EC-PSO). This embraced EC-PSO as CHs for choosing nodes close to the energy Centre. Nevertheless, EC-PSO is associated to network environments with even nodes as it uses geometric methods during the first cycle to obtain evenly distributed CHs.

PROPOSED MECHANISM

Secured Clustering is one of the most powerful strategies for safe and efficient data transfer within WSN. As communication happens from many sensors nodes and outside the mechanism which leads to many security issues in WSNs.Owing to the untrustworthy optimization in a local and global, these nodes face issues of communication abilities like the limited range and broad bandwidth probably limit the wireless communications in WSNs which becomes difficult for WSNs to operate with appropriately. One more issues is the security and privacy factor in which several sensors cannot prevent unwanted access and malicious attacks which leads to security breaches. The issue arises due to the communication ability and security as the cluster heads (CH) interacts with the neighbour nodes, nodes which are close to the base station, node coverage area. Hence secured clustering is very efficient technique for the secured and efficient communication in WSNs, keeping this security concern, to secure the wireless sensor networks (WSNs), we proposed a novel model called Secured Communication and Trust based protocol Model (SC-TBPM). In this model we will be focusing on the Security parameters like energy remaining(ER), density of node (DN), and average distance of cluster (ADC) by using a Whale swarm Secured clustering Algorithm (WSSC) mainly focuses on trust worthy nodes as cluster heads (CHs).

Our proposed SC-TBPM model is divided into the setup of network model; security model followed with the whale swarm secured clustering algorithm (WSSC) each of its representation is given in detailed below.

SC-TBPM Network Model

The system architecture is now seen as additional storage concept. It consists of a sensor, and a remote receiver, d. All Tx and Rx can be found on the amplifier circuits. The properties below concerning the WSN are stated:

1. Maximum sensor nodes are distributed evenly and stable.
2. Node is similar to homogeneous and has less power.
3.The BS is stationary and the sensing field may be located internally or externally.
4.Node collects data on a regular basis and has some data to forward.
5. A node doesn't really know where it is located or where other nodes are located.
6. The nodes must be self-organized and controlled after deployment.
7.The fusion of data is used to monitor the volume of data transmitted.
8.Each node is capable of operating as a head cluster.

The WSN scheme proposed for simulations has all of the features and disadvantages mentioned earlier. By measuring the signal intensity obtained the nodes determine the gap between both the transmitter as well as other networks.

SC-TBPM Security Model

The security model of our proposed methodology is designed below and it shows how it contributes in securing the communication happens without affecting the sensor nodes.

1.Clustering eliminates the effect of the route list situated at only the community points by having the routing setup inside the cluster and get range of the node.
2.Clustering can preserve network bandwidth from which size of cluster formation communications with CHs can be accomplished close to the base station nodes and avoids unwanted exchange of messages among sensor nodes.An optimal number of cluster heads (CHs) in a network is calculated by employing a probability based approach.
3.By using a probability dependent method an optimum number of cluster heads (CHs) in a network is determined.
4.Whale Swarm Secured Algorithm (WSSA) is used, based on the estimated performance of each cluster member, to pick the best node as a CH within each cluster.
5.Trust measures called packets successfully forwarded through a node and delay in transmission are regarded to select only a trustworthy and reliable node as CHs.
6. Node's fitness for the CH selection process is evaluated using the WHALE SWARM (Ω) based on three more parameters.
a.energy remaining(ER)
b.density of node (DN)
c.Average distance of cluster (ADC) for metrics ER and DN.
7.In this request a nearest neighbour criterion is used to luster WSN. This helps to reduce the communication range to the cluster.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

8.SC-TBPM aims to avoid choosing compromised nodes as CHs in order to create a stable network. It surpasses the current strategies by calculating the operating selection rate as CHs for compromised nodes.

WHALE SWARM SECURED ALGORITHM (WSSA) for SC-TBPM Model

INPUT- Security factors like energy remaining(ER), density of node (DN), average distance of cluster (ADC) for metrics ER and DN by using the WHALE SWARM (Ω)

OUTPUT- Secured trust worthy metrics

1. Start
2. Parameters initialization of energy remaining(ER), density of node (DN), average distance of cluster (ADC) for metrics ER and DN.
3. Initialization of whales position say as WHALE SWARM (Ω)
4. Evaluate fitness values of all whales.
5. Do it when the loop is stopped
6. For (j=1) the location of WHALE SWARM; |Ω| ; do
7. Get all the closest and finest location of the whales, tell Z of any; Ωj;
8. If there is closest and best stance of the whales (Z);
9. Whale location (Z) shifts under equation direction-(3)
10. WHALE SWARM prediction (almost) (Ω)
11. Ends the loop
12. For ends of the loop
13. The while loop ends
14. Revert the Secured trust worthy metrics
15. End

The common paradigm of WSSA using secured trust worthy metrics parameters of cluster head selection of SC-TBPM model is designed. Here we represent the trust metric parameters, whale positions etc. Before going in any iteration, each whale needs to find its ' ' best and nearest Secured trust worthy metrics whales as shown in algorithm.

WHALE SWARM SECURED CLUSTERING ALGORITTHM (WSSC) for SC-TBPM Model

Input- Secured Trust worthy Metrics and Whale Swarm (Ω)

Output-Secured Communication Parameters (Sc)

1. Starting
2. Parameter initialization
3. Whale initialization
4. Measure quality values of all whales
5. Review while loop; if not satisfied, during the termination loop
6. For (j=1) the location of WHALE SWARM;|Ω| ; do
7. Get the best and utmost place to interact with whales, say Z of all j;
8. If location of the whales (Z) exists then
9. Make a copy of say R(ABJ);
10. With respect to Z, R moves by the above
11. Expand R; Ωi.d=0;
12. If f(R) <f(Ωi)
13. Ωi=R;
14. Otherwise
15. Verify the loop counter Ωi;
16. Ends the loop
17. Otherwise
18. Verify the loop counter Ωi;
19. Ends the loop
20. For ends of the loop
21. the loop ends when Checking every whale is the best way to interact(Ω)
22. Return secured communication(sc)
23. end

Algorithm Iterative Counter for Whale

Requirements:

Whale solution (S), Stability level Ts

1. Starting
2. If (R.d#Ts)
3. Otherwise
4. Check R-about; Communication(sc) secured
5. Retrigger R;
6. Expand R;
7. End so if
8. Finish

Algorithm For Finding WSOA-MOCH Best Secured Communication

Requirements:

Solution (S); Threshold Fitness (T_f); $Trust_{optimization}=F_{combest;}$

1. Start
2. If $f(S)<f_{combest}$ then
3. If $f_{mulbest-}$ $f(S)>T_f$ then
4. Clear $trust_{optimization;}$
5. end if
6. $f_{globest=}$ f(S);
7. Add S to $trust_{optimization;}$
8. Else
9. If f(S)---- $f_{combest<=}T_f$ then
10. Add S to $trust_{optimization;}$
11. If loop ends
12. If loop ends
13. Finish

MATHEMATICAL MODEL FOR BEST SECURED COMMUNICATION

Communication Delays

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

Communication period was the estimated number required to drive the portion of a whole network in only a packets swap-focused device that would be the delays due by a bit rate. Communications delay is simply a packet length vector, and has nothing to do for both networks' range. Their pauses are often in proportion to the length of a packet.
The formulation is given as follows:

$C_d = \frac{NB}{RC}(seconds)$ (1)
Where Cd = Delays the communication in secs
NB = Bits Number
RC = Communication Rate
Combine the following devices capable of transmitting packets of data at various rates, and thus have different delays in communication. Communication delays are based on as:
Now let believe that contact delays are distributed dynamically and separately for two devices as 1 and 2 respectively with parameters μ1Δt and μ2Δt. The possibility that the communication of a packet by device 1 needs X time slots is given as
$P(d_{tr,1}=X\Delta_t)=\mu_1\Delta_t(1-\mu_1\Delta_t)^{X-1}$, X=1,2,3.... (2)

The possibility that perhaps the communication of packets by system 1 needs X time slots is provided as

$P(d_{tr,2}=X\Delta_t)=\mu_2\Delta_t(1-\mu_2\Delta_t)^{X-1}$,X=1,2,3.... (3)
Conclude that even a period t0 at system 1 will actually send a packets and the possibility that the packet will be sent at the period == $t_{0+}\Delta t$
Compute the probability
$P(t_0+d_{tr,1\leq t0}+\Delta_t)=P(d_{tr,1}\leq\Delta_t)$ (4)
Where $d_{tr}$is the Communication delay of the packet
$P(d_{tr,1}\leq\Delta_t)=P(d_{tr,1}=\Delta_t)=\mu_1\Delta_t$ (5)

So probabilities (dtr, 1 = Xt) P (dtr,2 = Xt) is that it takes X(t) times in P(dtr,1 = Xt) P(dtr,2 = Xt) chance to communicate the entire packet by system 1 itself. (Failure to send the packet (X−1)(X−1) twice and the last time to send it −1 + 1 = X)
$P(t_0+d_{tr,1\leq t0}+\Delta_t)=P(d_{tr,1}\leq\Delta_t)$ (6)

- Where t_0 ------->start of time Communication ;
- $d_{tr,1}d_{tr,1}$ ------->Packet time delay communications;
- $\Delta_{t1}\Delta_{t2}$ ------->One Time Slot Period;
- $t_0+d_{tr,1}$ ------->time that packet arrives;
- t_0+d_{tr+1} -------> time of Communication + Communication delay;
- $t_0+\Delta_{t1}$ ------->Newest average packet period;
- $t_0+\Delta_{t2}$ ------->time of Communication + one time slot;
- $\{t_0+d_{tr,1}\leqslant t_0+\Delta_1\}$If packets are interrupted no longer for one time frame after Contact starts. We're searching for the possibility of this occurring.
- $\{d_{tr,1}\leqslant\Delta_1\}$is the event that packet is delayed no longer than one timeslot.

$\therefore P(t_0+d_{tr,\,1\leq t0}+\Delta_t)=P(d_{tr,1}\leq\Delta_t)$ (7)
$\therefore P(t_0+d_{tr,\,1\leq t0}+\Delta_t)=P(d_{tr,1}\leq\Delta_t)$ (8)

We could compute the possibility of this occurrence. Both are expected to be the same occurrence as Contact delay is probably independent of communication time.
Secured Communication Load Probability
If x or y are now the reactive and active load elements at any stage we can measure the possibility of this protected load Contact events. It is defined with the equation below

$Z_i = S_{Di} = X_i + j_i$ (9)
Therefore the periods of loads of contact are determined by
$M_t(S_{Di}) + a_i^n S_{Di}{}^1 P_i$ (10)

Where m_t=moment of order
S_{pi}= Loading to unique node
P_i=probability of having S_{pi}

Simulation Results

Simulation Model and Parameters

In this paper work, we simulate a heterogeneous WSN network by using Network Simulator-3.25, by configuring network with different energy model and different network properties such as physical model and channel model. To determine the efficiency of proposed Whale Swarm secured clustering algorithm (WSSC), we configure the experiment by varying network topology by varying number of nodes. In this experiment we defined the various energy rates, and channel rates to the sensors to balance the overall performance. In this simulation we employed a different network topographies by representing the network size from 50 sensor nodes to 200 sensor nodes.
In this experiment we design a heterogeneous cluster network topology by configuring WSSC protocol module in NS2. The WSSC protocol optimizes the route and defines a routing packets to identifies the optimal routes. We compare our experimental study with Whale Swarm Algorithm with Iterative Counter (WSA-IC) [16].The simulation settings and parameters are summarized in Table 1.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 5, Issue 9, September 2020

Table I Simulation settings and parameters

Parameter	Value
Network Area	100m × 100m
Nodes number	50,100, 150, 200 nodes
Channel	Wireless
Phy	WirelessPhy
Routing algorithm	WSSC
Mobility Model	Constant Position
IP Address	IP4
MAC	802.11
Socket	UDP Socket Factory
Initial energy	0.5 J
BS location	(50,50)
Packet size	4000 bits
Simulation Time	50s

Results and Discussion

Fig. 2 represents the total number of packets transmitted to the receiver based on the number of nodes, the simulation results determines the packet delivery ratio of WSSC is increased when less number of nodes are presented in the network and slightly dropped with respective of number of nodes changed, while compare with WSSCA protocol the performance is slightly better compare to WSA-IC

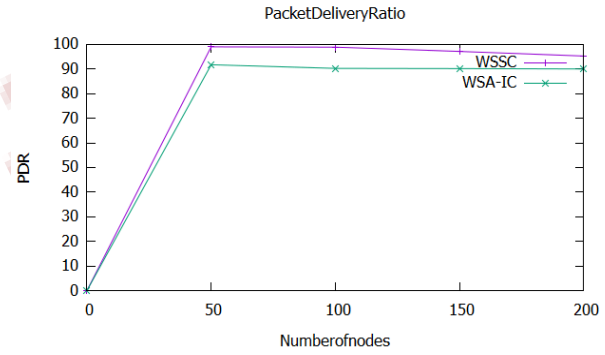

Fig. 2 Packet Delivery Ratio vs. Number of nodes

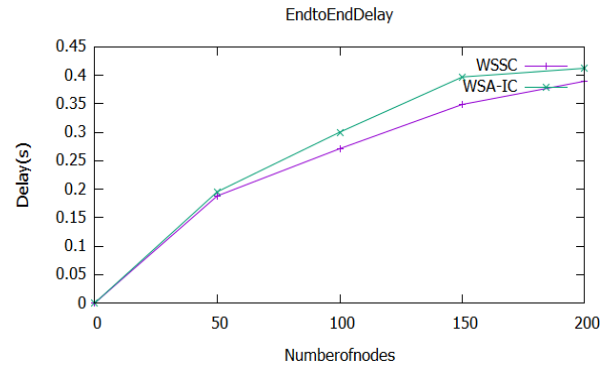

Fig.3 End-to-End Delay vs. Number of nodes

Fig. 3 Presents the end-to-end delay to reach to the base station based on the number of nodes, the above simulation results determines the delay of WSSC is increased with respective of number of nodes and the performance is slightly better compare to WSA-IC for different number of nodes

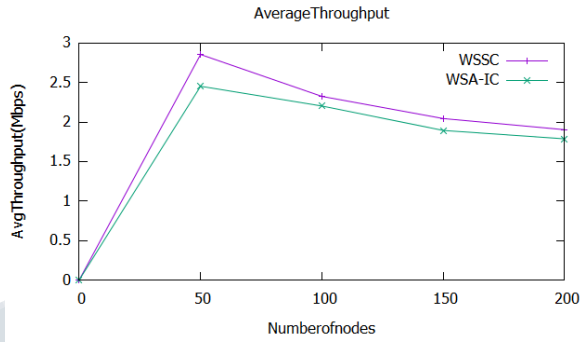

Fig. 4 Average Throughput vs. Number of nodes

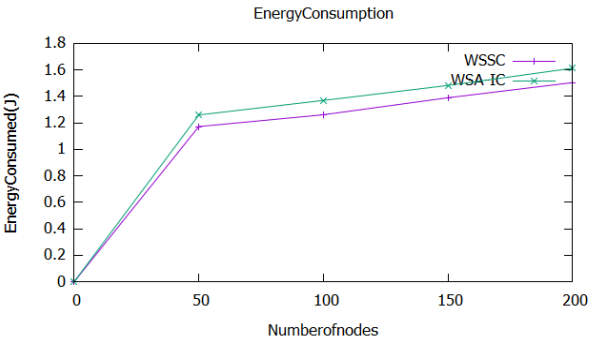

Fig.5 Energy consumption vs Number of Nodes

Fig. 4 and Fig. 5 represent the average throughput and energy consumption of both models performance by varying number of nodes. Hence, the energy consumption and throughput of WSSC is better than WSA-IC.

CONCLUSION

In WSNs, clustering is a useful technique to expand the network's lifetime as well as to protect each node in wireless sensor networks. Many issues with real-world optimization arise with multiple secure global and local communications. Owing to the untrustworthy communications faces issues like the limited range and broad bandwidth probably which becomes difficult for WSNs to operate with appropriately and one more issue is the security and privacy factor in which several sensors cannot prevent unwanted access and malicious attacks which leads to security breaches. The goal

of this study is to analyze and create a stable trust-based protocol model called the SC-TBPM model that uses whale swarm-secured clustering algorithm (WSSC) that focuses on trust-worthy nodes as cluster heads(CHs) by considering security parameters such as energy-residual (ER), node density (DN), average cluster distance (ADC).

REFERENCES

[1] Sharma, R., Vashisht, V., Singh, A.V., et al.: 'Analysis of existing clustering algorithms for wireless sensor networks' in Kapur, P., Klochkov, Y., Verma, A., et al. (Eds.): 'System Performance and Management Analytics. Asset Analytics (Performance and Safety Management)' (Springer, Singapore, 2018), pp. 259–277

[2] Ruan D, Huang J. A PSO-Based Uneven Dynamic Clustering Multi-Hop Routing Protocol for Wireless Sensor Networks. Sensors (Basel). 2019;19(8):1835. Published 2019 Apr 17. doi:10.3390/s19081835

[3] Sharma, R., Vashisht, V., Singh, U., et al.: 'Nature inspired algorithms for energy efficient clustering in wireless sensor networks'. Int. Conf. on Cloud Computing, Data Science and Engineering (Confluence), Noida, Uttar Pradesh, India, 2019, pp. 365–

[4] Juliana, R., Maheswari, P.U.: 'An energy efficient cluster head selection technique using network trust and swarm intelligence', Wirel. Pers. Commun., 2016, 89, (2), pp. 351–364

[5] Bayrakdar, M.E.: 'A smart insect pest detection technique with qualified underground wireless sensor nodes for precision agriculture', IEEE Sens. J., 2019, 19, (22), pp. 10892–10897, doi: 10.1109/JSEN.2019.2931816

[6] Bayrakdar, M.E.: 'Cooperative communication based access technique for sensor networks', Int. J. Electron., 2019, in press, doi: 10.1080/00207217.2019.1636313

[7] Arumugam, G.S.; Ponnuchamy, T. EE-Leach: Development of energy-efficient LEACH protocol for data gathering in WSN. EURASIP J. Wireless Commun. Netw. 2015, 2015, 1–9. [CrossRef]

[8] Yuea, J.; Zhang, W.; Xiao, W.; Tang, D.; Tang, J. Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks. Procedia Eng. 2012, 29, 2009–2015. [CrossRef]

[9] Pant,M.;Dey,B.;Nandi,S.Amulti-hop routing protocol for wireless sensor network based on grid clustering. In Proceedings of the 2015 Applications and Innovations in Mobile Computing (AIMoC), Kolkata, India, 12–14 February 2015; pp. 137–140. [CrossRef]

[10] Huang,J.;Hong,Y.;Zhao,Z.;Yuan,Y.Anenergy-efficientmulti-hoprouting protocol based on grid clustering for wireless sensor networks. Clust. Comput. 2017, 20, 3071–3083. [CrossRef]

[11] Ari, A.A.A.; Labraoui, N.; Yenké, B.O.; Gueroui, A. Clustering algorithm for wireless sensor networks: The honeybee swarms nest-sites selection process based approach. Int. J. Sens. Netw. 2018, 27, 1–13. [CrossRef]

[12] Yalçın, S.; Erdem, E. Bacteria Interactive Cost and Balanced-Compromised Approach to Clustering and Transmission Boundary-Range Cognitive Routing in Mobile Heterogeneous Wireless Sensor Networks. Sensors 2019, 19, 867. [CrossRef]

[13] Karaboga, D.; Okdem, S.; Ozturk, C. Cluster based wireless sensor network routing using artificial bee colony algorithm. Wirel. Netw. 2012, 18, 847–860. [CrossRef]

[14] Rao, P.C.S.; Jana, P.K.; Banka, H. A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks. Wirel. Netw. 2017, 23, 2005–2020. [CrossRef]

[15] Kuila, P.; Jana, P.K. Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. Eng. Appl. Artif. Intell. 2014, 33, 127–140. [CrossRef]

[16] Bing Zeng, Xiang Li, Liang Gao, Yuyan Zhang and Haozhen Dong, "Whale swarm algorithm with the mechanism of identifying and escaping from extreme points for multimodal function optimization", Received: 9 July 2018 / Accepted: 18 December 2018 Springer-Verlag London Ltd., part of Springer Nature 2019

[17] Wang J, Gao Y, Liu W, Sangaiah AK, Kim HJ. An Improved Routing Schema with Special Clustering Using PSO Algorithm for Heterogeneous Wireless Sensor Network. Sensors (Basel). 2019;19(3):671. Published 2019 Feb 7. doi:10.3390/s19030671