IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 12, No. 4, August, 2022, pp. 441-448
Journal homepage: http://iieta.org/journals/ijsse

CSCRT Protocol with Energy Efficient Secured CH Clustering for Smart Dust Network Using Quantum Key Distribution

Dennison Rajesh*, Gowda Shankarappa Rajanna

Computer Science and Engineering, Srinivas University, Mangalore 574146, Karnataka, India

Corresponding Author Email: rajeshd936@gmail.com

https://doi.org/10.18280/ijsse.120404

Received: 4 June 2022
Accepted: 16 August 2022

Keywords:
cluster head, CSCRT-chance succession comparison ratio, energy efficiency, IDS-intrusion detection system, quantum key distribution, routing protocol, WSN-wireless smart dust networks

ABSTRACT

Energy efficient protocols for Mobile wireless smart dust networks are getting prominence in the present scenario. This paper describes a novel scheme for intrusion detection framework for secured clustered mobile smart dust networks which better suits the periodical data gathering. The essential objective of a battery equipped mobile wireless smart dust nodes is to upgrade the transmission energy. The proposed protocol has the favourable position that the communication and computational overheads get reduced and gives improved energy efficient routing protocol as far as energy efficient and intrusion detection system. The intrusion and interruption are fundamentally same as that it is difficult to recognize. The design becomes more complex, any security protection algorithms utilize more energy. This can be achieved by using IDS based clustering tactic, Specific Encryption algorithm with Quantum Key Distribution and Chance Succession Comparison Ratio Test protocol. Particular encryption for data based communication is carried out to low utilization of energy and also to discover attacks, when it occurs in mobile nodes. Data transmission rate is a factor for energy utilization. Simulation is done in NS2, results show that better energy efficient routing scheme for mobile wireless smart dust network.

1. INTRODUCTION

A Mobile Wireless Smart dust Network (MWSN) can basically be characterized as a wireless smart dust network (WSN) in which the smart dust nodes are versatile. MWSNs are a littler, rising field of research rather than their settled antecedent. MWSNs are substantially more flexible than static smart dust arranges as they can be sent in any situation and adapt to quick topology changes. Not with standing, a significant number of their applications are comparative, for example, condition observing or reconnaissance. Normally, the nodes comprise of a radio handset and a microcontroller controlled by a battery, and in addition some sort of smart dust for identifying light, warm, moistness, temperature, and so forth [1, 2].

MWSNs have particular difficulties because of low transmission data transfer capacity, compelled control supplies, small memory sizes and, at long last, constrained energy [3], way of security arrangements cannot be directly connected to WSNs [4]. In this manner, new thoughts and approaches (protocols) are required keeping in mind the goal is to build security for MWSNs. In this paper, CSCRT Protocol with Energy Efficient Secured CH Clustering for MWSNs. Intrusion is an active or passive action in a network devoid of having authorization. Security system constitutes intrusion prevention and identification as first and second line of protection. Intrusion prevention systems cannot be stopped due to misbehaviour of illegalized person. In this way intrusion detection systems become possibly the most important factor. Clusters in MWSN illustrated in Figure 1. group of mobile smart dust nodes form cluster and cluster head (CH). CHs are capable of managing smart dust nodes, for example, node information, node energy, node lifetime, and data transferring.

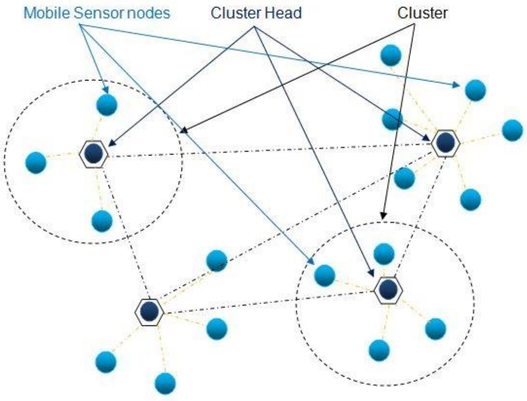

Figure 1. A clustered MWSN

2. RELATED WORK

In existing methods, numerous of energy awake approaches have been established for MWSNs. Energy effectiveness can be enhanced at different levels of the transmission approach for MWSN. While the mobility is established in the smart dust nodes, the topology suit very active, and the process of identifying the steady routes under such conditions become demanding. Additionally, it is impracticable for the MWSN nodes to survive up through the transparency of preserving routing tables mostly due to involved memory restrictions. Consequently, diverse table determined routing approaches for wireless networks are not straightforwardly appropriate to MWSN. SPEED [5], SAR [5] and Multi-path and Multi-SPEED routing approach MMSPEED [6] are a few routing approaches established for WSN, that can assemble the objectives like appropriate delivery of information packets. Low energy-adaptive clustering hierarchy LEACH [7], power efficient-gathering in smart dust information systems PEGASIS [8], threshold sensitive-energy efficient smart dust network TEEN [9], adaptive-TEEN [9], furthermore, these approaches which do not think about mobility of basestation and smart dust nodes. The modified-LEACH M-LEACH [10] is expansion of LEACH method can hold mobility of smart dust nodes. Though, M-LEACH does not think mobility in basestation. Energy-Efficient and Reliable-Routing (E^2R^2) for MWSNs think about the mobility of basestation and smart dust nodes while routing resolution are made, but less security while routing resolution [10, 11]. B92 utilizes non-orthogonal bases to transmit qubits to delivery side [12]. Quantum Key Distribution Protocol (QKDP) [13]. Therefore, none of the existing approaches can accomplish all the subsequent objectives at same occasion:

i. Trustworthiness in an energy resourceful behaviour in occurrence of smart dust node and basestation mobility.
ii. Organization mobility in smart dust nodes and preserving connectivity through alternating pathways.
iii. Diminish communication transparency.
iv. Detecting intrusion in smart dust nodes while entering or linking with the network.
v. Re-clustering time can be reduced.

Consequently, secured energy-efficient and trustworthy routing in MWSN setting is still a concern.

In this research work,

1. Mobility of basestation and smart dust nodes while routing resolution are made.
2. Conception of Assistant cluster head (ACH) is utilized, that enhances duration of network.
3. Conception of CH team is used, that enhances duration of network.
4. Conception of reaction by the basestation and smart dust nodes about information delivery.
5. Protocol guarantee trustworthiness in provisions of information delivery at the basestation and smart dust nodes, this is accomplished throughout the use of various routes and exchange of the path as determined by the basestation.
6. Detecting intrusion in smart dust nodes while entering or linking with the network.

Re-clustering time can be reduced, that enhances the duration of the network.

3. SYSTEM MODEL

The proposed IDS depends on multi-order secured energy efficient clustering, implying that first order CHs for CHs and subordinates for second order CHs. First order CH and second order CHs are shown in Figure 2. that is Second order CHs are assistant CHs for first order CHs. For the determination of the CHs, proposed work deals with residual energy, node lifetime availability aware secured clustering algorithm [14-16].

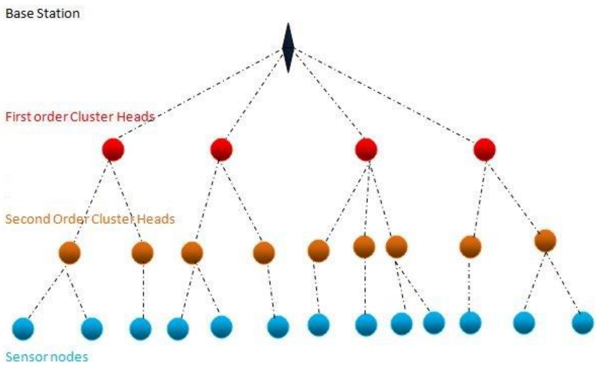

Figure 2. Proposed intrusion identification system

Selected First order and second order CHs have extreme hop value "1 & 2". Multi-order clustering illustrates two approaches of intrusion identification in MSWN.

i. Descending intrusion identification system (DIIS): CHs monitor lower order CHs and smart dust nodes activities by using watch dog mechanism and observing the activities performed by them are collected in an entry table [17].

ii. Ascending intrusion identification system (AIIS)*:* A specific number of monitoring was done, irregular action in CH is reported to upper order CH by subordinates CH [18].

Intrusions in the subordinate nodes and upper order CH identified by DIIS and AIIS.

3.1 Descending intrusion identification system

CHs hold watchdog counters with variation from the norm counters. Intrusion identification from CHs to subordinate identified as DIIS. For instance, consider system appeared in Figure 3. Node A defines first order CH and remaining of them are smart dust nodes initiate watchdog counter for subordinate smart dust nodes, specifically SN1, SN2, ..., SN6.

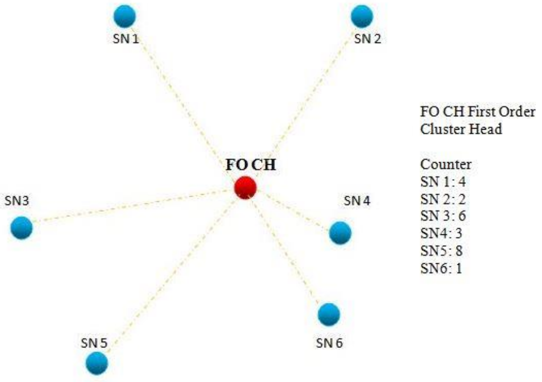

Figure 3. Watchdog counter for intrusion identification system

At whatever point any watchdog counter achieves a specific threshold. Specific threshold will be a maximum of 10. The smart dust nodes are flagged and included into entry table. Threshold breakage in smart dust node leads to node block and data drop, system appears in Figure 3. Assume SN5 contains watchdog counter of "10" and threshold level for watchdog counters is "10". Since watchdog counter of SN5 achieved threshold, SN4 is set apart as anomalous smart dust nodes in entry table, as mentioned in Figure 4. At that point, event transmission with SN5 gets blocked by first order CH at smart dust node A. Specified DIIS relevant to all order of cluster.

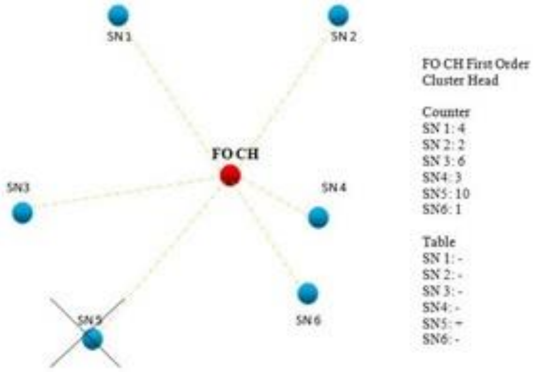

Figure 4. Entry table intrusion identification system

3.2 Ascending intrusion identification system

A specific number of monitoring was done, irregular action in CH is reported to upper order CH by subordinates CH. Irregular movement is resolved when the watchdog counter reaches a specific threshold. Aggregate estimation in irregular event is generated by sensible {OR,+} operation. Monitored watchdog OR'ed with whatever remains of watchdog output. Subsequently, last choice related with irregular conduct of CH is finished up by organized exertion of monitoring smart dust nodes. Methodology for utilizing OR'ed data as per the following: Sleep mode smart dust node miss unusual contact of CH in a particular time interval, other nodes in awake state. Individual monitoring of each smart dust nodes gets updated after specific time period.

Keeping in mind end goal to get a large portion of incidence high chance of identification, sleep/awake cycles in monitoring smart dust nodes allocated in likely manner. For instance, three monitoring smart dust nodes in a cluster and one in sleep state for particular time period, at that point event observed is left of monitoring smart dust nodes to be in awake state.

4. PROPOSED CSCRT APPROACH FOR MWSNS

4.1 Detection entities

Smart dust Nodes contain two categories of functionality, Sensing and direction-finding. Every smart dust node will sense the atmosphere and exchange information in among smart dust nodes and cluster nodes. Since smart dust nodes contain a large amount of resource restrictions.

Cluster Node performs as a supervise node for the particular smart dust nodes. One CH is allocated for every hexagonal region. It will collect the information from smart dust nodes, evaluate and combined the information and broadcast to regional node. It is more authoritative than smart dust nodes and has interruption recognition ability built into it.

Regional Node will supervise and collect the information from nearby CHs and transmit the mutual alarm to the higher level basestation. It is also a supervise node similar to the cluster nodes with the entire IDS functions. If hundreds of smart dust nodes are presented at the lower level subsequently the entire region will be dividing into a number of regions.

BaseStation is the highest element of construction authorized with human agent. It will collect the packets from regional nodes and dispense the data to the users related on their request [19].

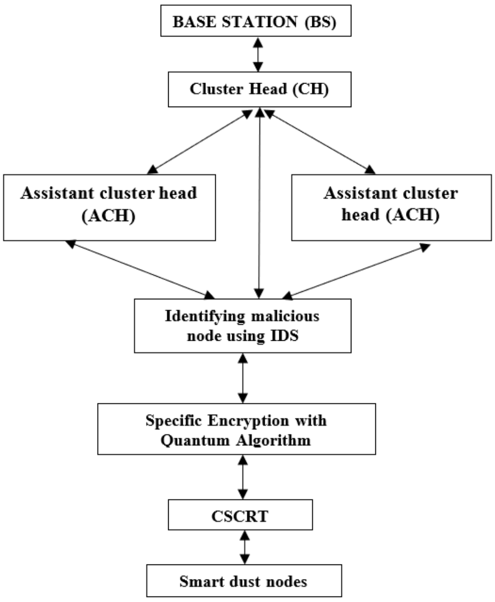
BASE STATION (BS)
Cluster Head (CH)
Assistant cluster head (ACH)
Assistant cluster head (ACH)
Identifying malicious node using IDS
Specific Encryption with Quantum Algorithm
CSCRT
Smart dust nodes

Figure 5. Proposed CSCRT approach

Smart dust nodes transfer the data from one smart dust node to the other smart dust node in multi hop fashion with the help of base station. The base station collects the data regarding the CHs and smart dust nodes in the cluster. The clustering phase the smart dust nodes select the CH having higher remaining energy evaluated to entire smart dust nodes in the cluster. Two assistant cluster heads (ACHs) are selected from the cluster. The smart dust node having subsequently minimum remaining energy is evaluated with CH and selected as ACH. In intrusion detection phase malicious nodes are identified in the network by IDS protocol. In IDS the basestation calculates the density of the smart dust node with threshold. Specific Encryption algorithm is to optimize the encryption algorithm for selected packets. If the node density is high when compared to every smart dust node in the network IDS identifies that smart dust node is malicious node and disconnected from network. To strengthens approach more efficient Quantum Key Distribution (QKD) technique applied to compute encryption and key sharing. The smart dust node with low density is considered to be normal smart dust node. Node density is a smart dust node requesting the basestation to connect with the network, which is a node frequently requesting to link with the network. Chance Succession Comparison Ratio Test is to identify mobile smart dust node can be authentic in the network. Figure 5 displays the architecture of CSCRT approach.

A Specific Encryption algorithm intends to achieve adequate improbability in the arrangement. Throughout the procedure of transmitting information, the smart dust node will arbitrarily generate a rate to specify the encryption amount which signifies amount of information will be encrypted between the broadcast information. After that a function is selected by the sender is previously deterministic number of information to encrypt. The specific encryption algorithm combines stochastic approach to enhance the ambiguity in the procedure of information selection. The other hesitant the encryption procedure is, the secure information transmission is related on the hypothesis that enough information is encrypted to grant trustworthy and explicit goal is to enhance key distribution scheme by implementing quantum methodology. CSCRT for the recognition of discriminatory forwarding attacks in network layer of MWSNs. This approach identifies premeditated information drops through high possibility recognition. Consequently, any dropped information attack towards protection of MWSNs.

4.2 IDS algorithm for clustering in MWSN

1. Begin
2. Creation of smart dust nodes
3. Organize a node in cluster infrastructure with source and BS.
4. Evaluate quantity of energy for all mobile nodes.
5. Evaluate quantity of density for all mobile nodes.
6. Decide weights w1, w2, w3 it depends on purpose. But w1,w2,w3 > 0
7. After that CH is elected based on its residual energy.
8. After selecting the CHs, two ACHs are elected from cluster by CH.
9. After ACHs are elected in each cluster broadcast starts in every cluster, where CH gathers information and shortest path from its particular mobile smart dust nodes MSNs.
10. While gathering information for MSNs, CH uses Induction Detection System IDS to its particular mobile smart dust nodes MSNs by means of node density and QKD algorithm.
11. If mismatching not found in decrypt data of (QKD) and the density of node is lesser than the computed density level the MSN will be connected to the CH.
12. Otherwise
13. MSN will be indicated as red and cannot be connected to CH.
14. Finally CH to BS.
15. End

4.3 Algorithm for specific encryption

Specific algorithm is observed to be an optimized encryption algorithm for selected packets. This included the following three stages:

1) The sender S will first put a random generator to arbitrarily acquire an encryption proportion ‘er’. Random generator is a computational device that will produce an arrangement of numbers or symbols that cannot be predicted. It is likewise imperative that requires security is given. SR is the Minimum threshold level encryption proportion that should reach by system. The sender S needs to find the encryption possibility. The activity is done through a capacity function to create an encryption possibility ‘pi’.

2) Following the means sender chooses the messages to encrypt. This enhances vulnerability in arrangement of which message will be encrypted and which are most certainly or not. The more vulnerability in system will preserve more secure communication [20].

Following algorithm is for specific encryption,
where,

Stage 1: Loop starts from incoming packets.

Stage 2: To calculate Entropy of the message. The entropy is a measure of data contained in message in the form of logical.

Stage 3: Updating the message Threshold value in three ways.

Case1: Message under assessment is the First message. At that point Threshold value of message is equivalent to Entropy.

Case 2: Message encryption rate is under 50 p.c. At that point Threshold value of message should 10p.c. Threshold value of message =previous calculated threshold value-current threshold value.

Case 3: Message encryption rate is higher than 50 p.c. At that point Threshold value of message should 10 p.c. Threshold value of message =previous calculated threshold value-current threshold value.

Stage 4: Message is encrypted if,

Entropy of the Message>= threshold value of the message. Else, encryption cannot take place.

Stage 5: Calculate the Encryption rate.

Stage 6: Continue until all messages are been processed.

The above mentioned algorithm enhances the vulnerability of the encryption and enhances the security by making the attacker to decrypt by QKD.

4.4 Algorithm for QKD

In this environment engages several smart dusts in key sharing process. To enhance key sharing technique by executing quantum methodology in specific encryption process by means of public key cryptosystem that enhances user validation and data reliability procedure. Furthermore no necessity of physical environment to verify the Qubits series, quantum technique distributes by applying asymmetric key sharing technique. It includes of two segments, (i). User Validation and Quantum Bases sharing, (ii). Data transmission over Quantum channel.

Since Smart dust node (SN) and CH to achieve a session key is for specific encryption algorithm.

4.4.1 User validation and quantum bases sharing

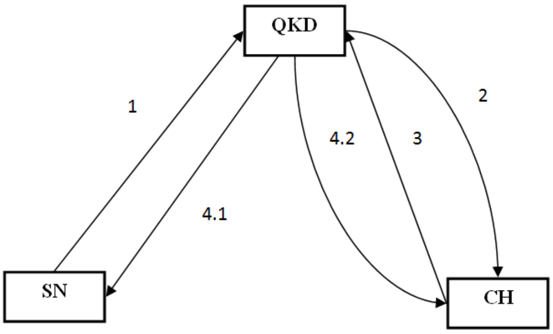

Figure 6. User validation and quantum bases sharing

1. SNs requests to join with CH

SNs ->QKD: $E_{PR-SN}(ID_{SN}|| ID_{CH})$

QKD force record the join request condition in log file and verify ID of SN for validation. Furthermore QKD verifies CH ID condition (Active, Free). If CH is free QKD shifts to subsequently step 2.

2. QKD sends to CH a join request including SN request

QKD ->CH: $E_{PU-CH}(ID_{SN} || ID_{CH})$

3. After CH respond by accepting join with SN, CH will transfer authorization call to QKD

CH ->QKD: $E_{PR-CH}(ID_{SN} || ID_{CH})$

QKD decrypts call and includes join condition among SN and CH and authentic to broadcast and obtain data.

4. QKD continues to issue quantum bases (+,X) in series to encode data to SN and CH in an encrypted data utilizing their public keys. After that,

4. 1 QKD->SN: $E_{PU-SN}(ID_{SN} || ID_{CH} || QB)$.

4. 2 QKD->CH: $E_{PU-CH}(ID_{SN} || ID_{CH} || QB)$.

Figure 6 shows steps involved in User Validation and Quantum Bases sharing.

4.4.2 Data transmission over Quantum channel

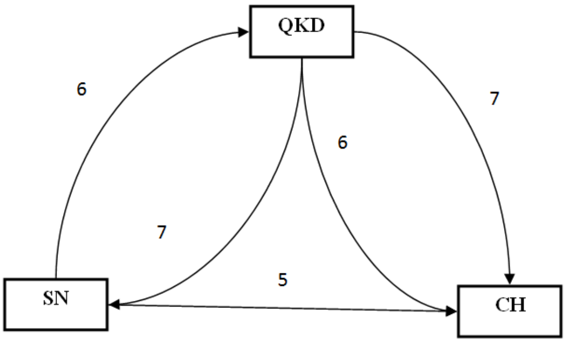

Figure 7. Data transmission over quantum channel

5. After SN and CH delivers quantum bases from QKD SN broadcast an encrypted data applying the quantum bases to CH

SN->CH: $E_{PR-SN}(E_{QB}(D)||E_{PU-CH}(ID_{SN}))$

6. CH and SN transmit a arbitrary region of data to QKD by applying Private Key of transmitter (SN, CH).

CH->QKD: $E_{PR-CH}(E_{QB}(D)||E_{PU-QKD}(ID_{CH})$

SN->QKD: $E_{PR-SN}(E_{QB}(D)||E_{PU-QKD}(ID_{SN}))$

QKD decrypt data and evaluate among them. Any mismatching found in bits subsequently QKD terminated there is malevolent.

7. QKD broadcast announcement data to SN and CH to notify them there is malevolent or not.

QKD->CH: E_{PU-CH} (E_{QB}(Indicated as red))

QKD->SN: E_{PU-SN}(E_{QB}(Indicated as red))

Figure 7 shows steps involved in Data transmission over Quantum channel.

If Indicated message is not a red is Okay link is active until QKD broadcast any fault message or SN discontinue broadcasting. Entire data is authentic by transmitter applying its private key. Furthermore data validation improvement is accomplished when smart dusts broadcast arbitrary region of data to QKD and identify them. By utilizing this approach able to eliminate guessing theory utilized in existing approaches as B92 [21], EPR [22] and BB84 [23], and better capability to recognize malevolent smart dust [24, 25].

4.5 Chance succession comparison ratio test

As indicated by CSCRT, an arbitrary variable u is utilized to characterize the status of data sending, where 0 signifies productive transmission of data and 1 means a data drop. u is ascertained as level of dropped packets verses data broadcasted. u' is characterized as satisfactory likelihood of dropped packets. Mobile smart dust node is represented authentic if u<= u' holds, and denoted as fake nodes if u > u' holds. u_0 < u' < u_1 characterizes the *gray area* for the decision making, where the choice is uncertain with respect to the authenticity of smart dust node.

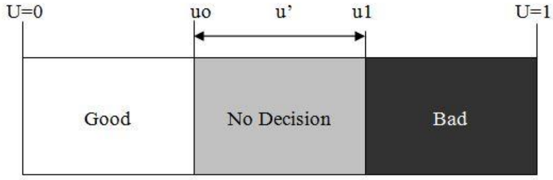

Figure 8. Decision making threshold

Assume 1, 2,…s signifies sample count. Decision made as displayed in Figure 8. Objective is to diminish the negative alarm rate, $a=U0(|D_s=1)$, and the neglect recognition rate, $r=U1(|D_s=0)$ Ds is decision at s samples, U0 indicates the broadcasted packet reached profitably and U1 indicates packet is not reached that a failure occurs. Whereas, (D_s = 1) the decision is positive of the CSCRT for packet broadcast and (Dm =0) the decision is negative of the CSCRT for packet is dropped. To achieve minimal quantity of samples s_{min}. CSCRT determines this value in Eq. (1),

$$s_{min}=(L(u)\log(a)+(1-(L(u))\log(r))/(u\log(u1/u0)+((1-u)\log((1-u1)/(1-u0)) \tag{1}$$

where, L(u) is determined in Eq. (2),

$$L(u) =(((1-a)/r)^{l}-1)/(((1-a)/r)^{l}-((1-r)/a)^{l}) \tag{2}$$

'l' can be resolute by Eq. (3),

$$u =(1-((1-u1)/(1-p0)^{l}))/((u1/u0)^{l}-((1-u1)/(1-p0)^{l})) \tag{3}$$

Accumulating s samples and all factors (u0,u1,a,r), threshold reception (T_{rec}) and threshold rejection (T_{rej}) evaluated in Eqns. (4) and (5) correspondingly,

$$T_{rec}=(\log(a/(1-r)))/((\log(u1/u0))-(\log(1-u1)/(1-p0)))+s(\log((1-u0)/(1-u1)))/((\log(u1/u0))-(\log(1-u1)/(1-p0))) \tag{4}$$

$$T_{rej}=(\log((1-a)/r))/((\log(u1/u0))-(\log(1-u1)/(1-p0)))+s(\log((1-u0)/(1-u1)))/((\log(u1/u0))-(\log(1-u1)/(1-p0))) \tag{5}$$

d_s is amount of packets dropped in s quantity of samples. CSCRT desires incessantly executed in Eq. (6),

$$T_{rec}<d_s<T_{rej} \tag{6}$$

Every cycle CSCRT has three probable results based on Eq. (6).

1. If **$d_s \leq T_{rec}$**, then smart dust node is genuine.
2. If **$T_{rec}<d_s<T_{rej}$**, then CSCRT continues.
3. **$T_{rej} \leq d_s$,** then smart dust node negotiation.

4.6 CSCRT decision making

As indicated in the study of Rais et al. [8], the decision making over an activated alarm concludes any one decision.

i) Intrusive, yet regular that is positive, interruption in system, however intrusion identification system unable to identify it and decide that event to regular one.

ii) Original smart dust node, yet irregular that is negative, no interruption in system, intrusion identification system erroneously closes a typical event to irregular one.

iii) Original smart dust node and regular that is negative, no interruption in system, and intrusion identification system finalizes that the event to be regular one.

iv) Intrusive and irregular that is positive, an interruption in system, and intrusion identification system finalizes that the event to be irregular one.

5. SIMULATION RESULTS AND ANALYSIS

Simulations are performed using NS2 offers an interactive location for the operation of algorithms, packet delivery, Packet Loss, End to End Delay, Residual Energy, Security. To simulate proposed routing approach, mixed smart dust nodes are arbitrarily organized. The energy effectiveness of the proposed secured clustering protocol for MWSN is analyzed through simulation results. Table 1 shows the parameters and values used during the simulation. Results of CSCRT is compared with EHCA [20].

Table 1. Parameters of simulations

Parameter	Value
Network region	150 × 150
Number of nodes	100
BS location	(75, 150)
Initial energy	1 J
Packet size	100 bytes
Number of rounds	150

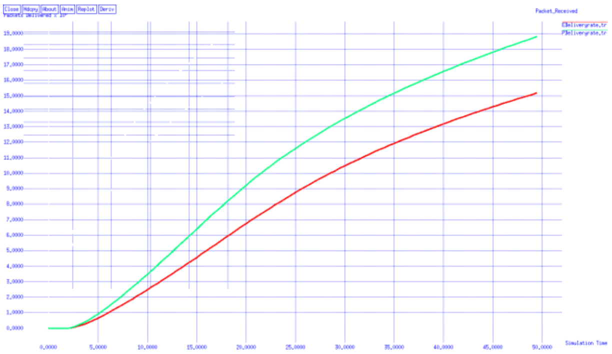

Figure 9. Packet received versus duration of mobile nodes

Figure 9 demonstrates the throughput for both existing EHCA and proposed CSCRT approach. For every cycle, the consequent throughput values are plotted. Throughput is the normal rate of successful information delivery over a broadcasting channel. This information may be delivered over multi hop network smart dust nodes. This is the amount of information received quickly as target user is able to receive information. The green line illustrates proposed method and the red one signifies the existing approach. It is comprehensible that throughput of proposed method is improved than existing tactic.

Figure 10 demonstrates the packet loss for the existing EHCA and proposed CSCRT approach. For every cycle, the consequent packet loss values are plotted. Packet loss is unsuccessful information delivery over a broadcasting channel. This is the amount of information loss to target mobile smart dust is unable to receive information. The green line illustrates the proposed method and the red one signifies the existing tactic. It is comprehensible that packet loss of proposed method is reduced than existing tactic.

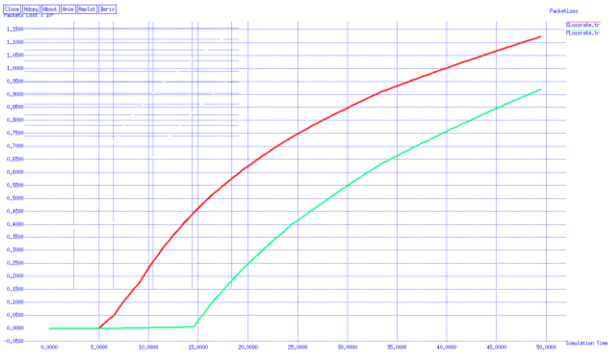

Figure 10. Packet loss versus simulation time of mobile nodes

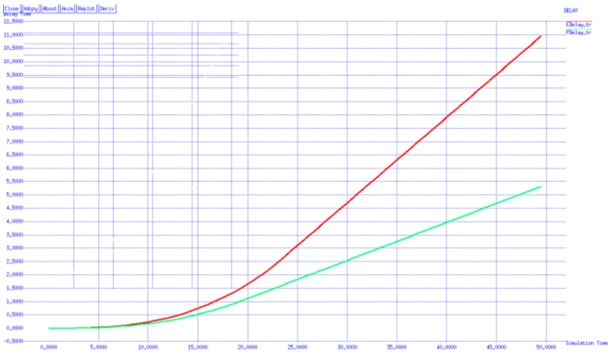

Figure 11. Average end to end simulation delay in mobile nodes

Figure 11 illustrates the delay for the existing EHCA and proposed CSCRT approach. For every cycle, the consequent delay values are plotted. The delay is evaluated in terms of the number of cycles and the delay in delivering the information to the basestation. The red one signifies the delay of the existing method and the green line illustrates the delay of the proposed approach. It is comprehensible that delay in proposed approach is reduced than existing tactic. Thus the proposed approach successfully minimizes the delay in delivering information to the basestation.

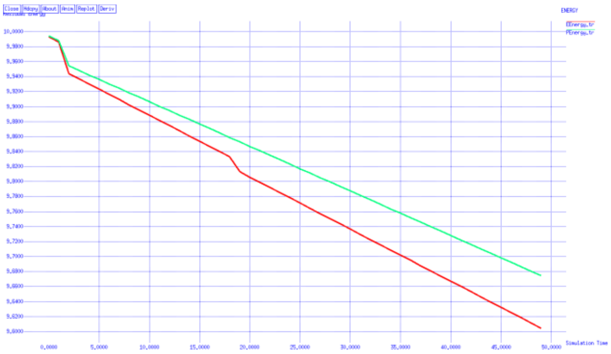

Figure 12. Residual energy to increase the duration of network

Figure 12 demonstrates remaining energy for the existing EHCA and proposed CSCRT approach. The energy utilized by the smart dust nodes is evaluated and the values are plotted. For every cycle, the consequent energy levels are plotted. The green line illustrates the proposed approach and red one signifies the existing approach. It is comprehensible that remaining energy of proposed approach is increased than existing tactic.

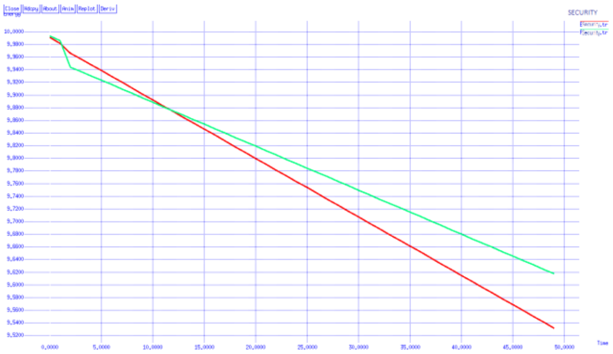

Figure 13. Increase of security simulation in mobile nodes

Figure 13 demonstrates security for the existing EHCA and proposed CSCRT approach. The mobile smart dust nodes get connected and disconnected from the network due to loss in energy, so the eavesdropper enters in to the network and they can make intrusion. For that interruption an intrusion identification system is adapted. For every cycle, the consequent security levels are plotted. The green line illustrates the proposed approach and red one signifies the existing approach. It is comprehensible that the security level of proposed approach is higher than the existing tactic.

6. CONCLUSION

In this research work a novel energy efficient secured clustering protocol CSCRT for MWSNs. The objective of routing protocols is not only to improve the network lifetime but also to reduce end to end delay, efficient throughput level, packet loss, better secure routing, better intrusion identification system and routing management. The consummation of the proposed method is evaluated with EHCA during simulation. A success to capitalize on the duration of networks up to 8% and security level up to 9% compare to existing approach EHCA. In future malicious nodes can be identification with a secret key Quantum Key Distribution methodology that provides enhanced energy proficient routing for mobile nodes.

REFERENCES

[1] Gowthami, K., Ramya, T., Sunil Kumar, M. (2017). A study on routing protocols and mobility models in mobile ad hoc networks. International Journal of Advanced Computational Engineering and Networking, 5(8). http://iraj.doionline.org/dx/IJACEN-IRAJ-DOIONLINE-9022.

[2] Chéour, R., Jmal, M.S., Khriji, S., El Houssaini, D., Trigona, C., Abid, M., Kanoun, O. (2022). Towards hybrid energy-efficient power management in wireless sensor networks. Sensors, 22(1): 301. https://doi.org/10.3390/s22010301

[3] Kandula, L.R.R., Lakshmi, T.J., Alla, K., Chivukula, R. (2022). An intelligent prediction of phishing URLs using ML algorithms. International Journal of Safety and Security Engineering, 12(3): 381-386. https://doi.org/10.18280/ijsse.120312

[4] Ashween, R., Ramakrishnan, B., Milton Joe, M. (2020). Energy efficient data gathering technique based on optimal mobile sink node selection for improved network life time in wireless sensor network (WSN). Wireless Personal Communications, 113: 2107-2126. https://doi.org/10.1007/s11277-020-07309-y

[5] Jigisha, P., Purushotham, A., Usha Rani, G. (2015). Research and improvement of sleep mode scheduling of routing protocol LEACH using TEEN, APTEEN in WSNs. IJREAT International Journal of Research in Engineering & Advanced Technology, 3(2). http://www.ijreat.org/Papers%202015/Issue14/IJREATV3I2028.pdf.

[6] Mishra, B., Rai, S.S., Saluja, N.K. (2015). M-LEACH: A modified version of LEACH for WSNs. In JETIR, 2(12): 82-87.

[7] Patel, G., Nirav, M.R. (2014). Routing protocols to provide quality of service in wireless sensor networks. Int J Res Adv Technol, 2(2): 14.

[8] Rais, A., Bouragba, K., Ouzzif, M. (2019). Routing and clustering of sensor nodes in the honeycomb architecture. Journal of Computer Networks and Communications, 2019: 4861294. https://doi.org/10.1155/2019/4861294

[9] Butun, I., Ra, I.H., Sankar, R. (2015). PCAC: power-and connectivity-aware clustering for wireless sensor Networks. EURASIP Journal on Wireless Communications and Networking, 2015(1): 1-15. https://doi.org/10.1186/s13638-015-0321-6

[10] Kaur, N., Sood, S.K. (2015). An energy-efficient architecture for the Internet of Things (IoT). IEEE Systems Journal, 11(2): 796-805. https://doi.org/10.1109/JSYST.2015.2469676

[11] Giji Kiruba, D., Benita, J. (2022). A survey of secured cluster head: SCH based routing scheme for IOT based mobile wireless sensor network. ECS Transactions, 107(1): 16725. https://iopscience.iop.org/article/10.1149/10701.16725ecst/meta.

[12] Rajesh, D., Kiruba, D.G. (2021). A probability based energy competent cluster based secured CH selection routing EC2SR protocol for smart dust. Peer-to-Peer Networking and Applications, 14(4): 1976-1987. https://doi.org/10.1007/s12083-021-01144-z

[13] Yang, T., Mu, D., Hu, W., Zhang, H. (2014). Energy-efficient border intrusion detection using wireless sensors network. EURASIP Journal on Wireless Communications and Networking, 2014: 46. https://doi.org/10.1186/1687-1499-2014-46

[14] Gavali, V.N. (2015). Anomaly network intrusion detection: A review. International Journal of Innovative Research in Advanced Engineering (IJIRAE), 2(4): 90-95.

[15] Butun, I., Ra, I.H., Sankar, R. (2015). An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks. Sensors, 15(11): 28960-28978. https://doi.org/10.3390/s151128960

[16] Sarma, H.K.D., Mall, R., Kar, A. (2015). E^2R^2: Energy-efficient and reliable routing for mobile wireless sensor networks. IEEE Systems Journal, 10(2): 604-616. https://doi.org/10.1109/JSYST.2015.2410592

[17] Shivani, R.K., Sheetal, A. (2015). SPEED a real-time routing protocol in wireless sensor networks. International Journal of Research in Advent Technology, 3(6). https://ijrat.org/downloads/Vol-3/june-2015/paper%20ID-36201515.pdf.

[18] Rajesh, D., Jaya, T. (2022). Energy competent cluster-based secured CH routing EC2SR protocol for mobile

wireless sensor network. Concurrency and Computation: Practice and Experience, 34(1): e6525. https://doi.org/10.1002/cpe.6525

[19] Kiruba, G. (2021). Energy capable clustering method for extend the duration of IoT based mobile wireless sensor network with remote nodes. Energy Harvesting and Systems, 8(1): 55-61. https://doi.org/10.1515/ehs-2021-0006

[20] Rahate, G., Chopade, N. (2022). Realistic vertical handoff predictive trigger thresholding in heterogeneous networks. Ingénierie des Systèmes d'Information, 27(4): 557-563. https://doi.org/10.18280/isi.270405

[21] Ismail, A.S., Wang, X., Hawbani, A., Alsamhi, S., Aziz, S.A. (2022). Routing protocols classification for underwater wireless sensor networks based on localization and mobility. Wireless Networks, 28: 797-826. https://doi.org/10.1007/s11276-021-02880-z

[22] Al-Bzoor, M., Musa, A., Alzoubi, K., Gharaibeh, T. (2022). A directional selective power routing protocol for the internet of underwater things. Wireless Communications and Mobile Computing, 2022: 3846621. https://doi.org/10.1155/2022/3846621

[23] Sarath, R., Nargunam, A.S., Sumithra, R.P. (2012). Dual channel authentication in cryptography using quantum stratagem. In 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1044-1048. https://doi.org/10.1109/ICCEET.2012.6203880

[24] Ahmad, R., Wazirali, R., Bsoul, Q., Abu-Ain, T., Abu-Ain, W. (2021). Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime. Sensors, 21(14): 4821. https://doi.org/10.3390/s21144821

[25] Kiruba, D.G., Benitha, J. (2014). Fuzzy based energy proficient secure clustered routing (FEPSRC) for IOT-MWSN. Journal of Intelligent & Fuzzy Systems, (Preprint), 1-13. https://doi.org/10.3233/JIFS-212014