AN EFFICIENT AND SECURE MALICIOUS NODE DETECTION MODEL FOR WIRELESS SENSOR NETWORKS

Asmaa M.Morsi[1], Tamer M. Barakat[2] and Ahmed Ali Nashaat[2]

[1]Electronics and Communications Department, Al-Madina Higher Institute for Engineering and Technology, Giza, Egypt
[2]Electrical Engineering Department, Faculty of Engineering, Fayoum University, Egypt

ABSTRACT

In wireless sensor networks (WSNs), there are many factors, such as the reciprocal interference of wireless links, battlefield applications and nodes are exposed to poor physical protection medium. All of these result in the sensor nodes being more exposed to be attacked and compromised. Since sensors are normally energy limited in WSNs, it is constantly basic to conserve the node energy and expand the lifetime of the network. Besides, hierarchical clustering is deemed as one of the numerous ways to deal with the reduction of energy consumption of nodes and increasing the network lifetime in WSNs. This paper conspicuously introduces an efficient and secure malicious node detection model based on a hybrid clustering network for WSNs (ESMCH) which is based on a trusted mobile node. WSNs are still suffering from some attacks like Man-in-the-Middle Attack and Black hole Attack, so by using the ESMCH model, we can avoid these attacks. Finally, simulation results also indicate that the proposed model can increase the network lifetime, and achieve an efficient and secure clustering network.

KEYWORDS

Wireless sensor networks, ESMCH, Clustering, Balanced Load, Fuzzy System and Energy.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have the countless number of inexpensive and small sensor nodes composed of many autonomous, battery-powered nodes. These sensor nodes are interconnected and dabbled together over a large area to sense and gather various data such as temperature, pressure, and humidity and can be used in many applications like animal tracking and biomedical applications [1]. Extraction of valuable information from an enormous amount of data needs, for high processing and computation, to be implemented at the sensor nodes. Wireless sensor nodes are randomly installed and communicate themselves through the wireless communication medium. It has few restrictions like limited energy, storage, and processing capabilities. A sensor node is a small and simple device with limited computational resources. These nodes suffer from limited battery power, limited of the resources and computational power. All of these result in the sensor nodes being more exposed to be attacked and compromised. Since sensors are usually energy limited in WSNs, it is always critical to conserve the node energy and extend the network lifespan that characterized as the time elapsed since the start of the network until the first sensor runs out of the energy. Besides, hierarchical clustering is deemed as one of the numerous ways to deal with the reduction of energy consumption of nodes and increasing the network lifetime in WSNs. Dividing the sensor networks on WSN into small controllable units is known as the clustering and the process known as clustering process. Though the main reason

behind the implementation of the clustering approach is to enhance the scalability of the network (prolong), it is an imperative factor for achieving an energy-efficient routing of the data in the network [2].

In wireless sensor networks (WSN), the current cluster-based routing techniques may result in increased network workload, energy consumption and re-transmissions [3]. In order to overcome these issues, we propose an efficient and secure malicious node detection model based on a hybrid clustering network for WSNs using trusted mobile nodes. In this model, each cluster node member sends the data to the cluster head. The aggregated data from the cluster head (CH) is transmitted to the base station through another cluster head called Super Cluster Head (SCH). An energy-efficient routing protocol is also developed based on the parameters expected the number of retransmissions and link failure probability.

The remaining of this paper is sketched as follows. Section 2 describes the related work in the field. Section 3 presents our system model and has some subsections which talked about used algorithms and the energy and security mechanisms. Section 4 presents the simulation results and discussion and finally, the conclusion is presented in Section 5.

2. RELATED WORKS

Jin-Shyan Lee and T. Kao developed an Improved Three-Layer Low-Energy Adaptive Clustering Hierarchy for WSNs. The authors developed this model to improve the energy and increase the lifetime of the network. This paper is fully concentrated on reducing energy consumption and prolonging the lifespan of WSNs. This is the disadvantage of this paper also by introducing the LEACH protocol, the performance level is insufficient. The simulation result shows the better performance when compared to others [2].

A survey on a Secure Data Aggregation for Wireless Sensor Networks using Double Cluster Head Approach introduced by A.L. Sreenivasulu and P. Chenna Reddy discussed double cluster head based secure aggregation method (DCSDA). In this paper, authors are concentrated on achieving security as the main aim which is appropriately applicable for the cluster-based communication approach. Also, it can deal with the privacy and authentication. The performance of the DCSDA system has been shown in the experimental calculation is in terms of energy consumption, packet drop ratio and delay [4].

Behara et al. introduced an Energy-efficient modified LEACH protocol for IoT application. An existing system, a threshold limit for the cluster head selection is introduced through changing the clustering protocol as alow-energy adaptive clustering hierarchy (LEACH). To increase the WSN lifetime, the performance of the modified LEACH protocol rises 67% in throughput. The performance of the LEACH protocol is much better when compared with other energy-efficient protocols. Additionally, the simulation shows the symbolic development in terms of stability period and network lifetime in various matrices such as area, energy, and node density [5].

I.S. Akila and R. Venkatesan proposed a model based on Fuzzy Based Energy-aware Clustering Architecture for Cooperative-Communication in WSN. For cooperative communication in WSN, Fuzzy-based clustering architecture is introduced. This algorithm is used to increase the energy-efficiency and to prolong the lifetime of the network. Here, the fuzzy-based clustering protocol is used to determine the cooperative node which combines the cluster. To establish the optimum path between each CN and CH data transmission, particle swarm optimization is used. To enhance the lifetime network and energy efficiency the proposed technique is used and the result shows in the simulation[6].

In [7] , a secure system is proposed that is based on Using Elliptic Curve Cryptography based Digital Signature Algorithm (ECCDSA) the nodes of this network will authenticate successfully; wireless sensor network security will indicate the security over the network by Node authentication, self-healing and Error correction process.

A new scheme known as Energy Efficient Clustering Scheme for Prolonging the Lifetime of WSN with Isolated Nodes has been introduced by JenqLeu et al. they proposed a good algorithm to reduce the energy consumption and prolonging the network lifetime (REAC-IN). The regional average energy and distance between sensors are used to enhance the lifespan of the WSN network and to be isolated from CHs. The simulation result shows the better performance when compared to others [8].

Hierarchical Clustering-Task Scheduling Policy in Cluster-Based WSN is proposed to achieve an energy-efficiency, more flexible and scalable clustering-task scheduling, the hierarchical clustering-task scheduling policy in a cluster-based algorithm (HCSP) is used. Each cluster is reconfigurable only once at each local super round based on HCSP. Hence, throughout the network, it may lead to differ from one cluster to another[9].

3. ESMCH MODEL

This model will be classified according to clustering head selection, the energy model and security mechanism.

3.1 Network Definition

The network consists of one cluster head. Other nodes are sub-divided into sub-clusters. Each cluster in the network consists of some main nodes as cluster head node (CH), child nodes (CN) and mobile nodes (MN). The cluster head node suffers from transferring the data directly to the Super-cluster head (SCH) due to the distance. To address these issues, mobile sink nodes are introduced. The mobile sink mode acts as an intermediate between the cluster head and Super-cluster head as shown in Figure 1. Each cluster has one or more mobile sink nodes consistent with the number of child nodes located in the cluster head.

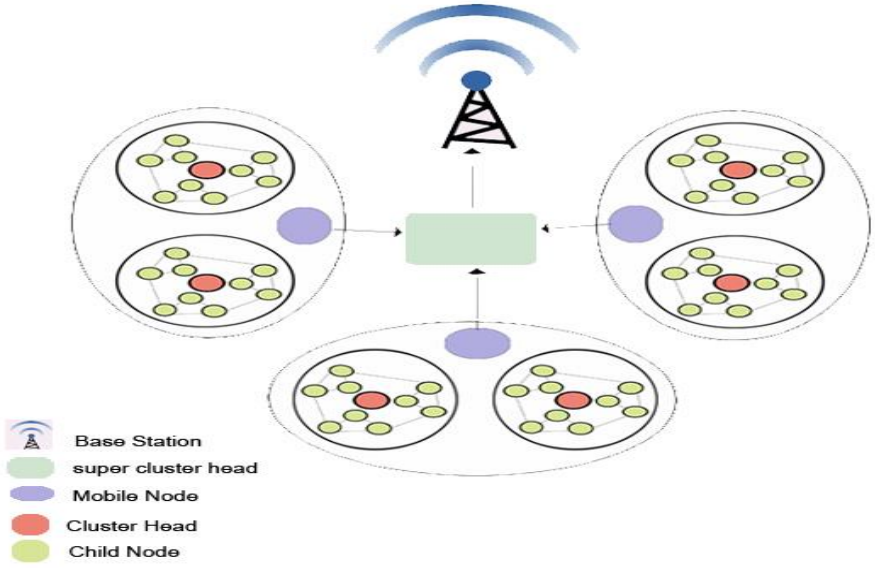

Figure 1: The Proposed Model of WSN

3.2. Proposed Cluster Head Selection Technique

In this research, the ESMCH proposed two algorithms named as Intelligent based Secured Fuzzy Clustering algorithm (ISFC) and Balanced Load Sub-cluster head selection to decrease the distance between the nodes and reduce energy consumption.

3.2.1 Balanced Load Cluster Head Selection

Balancing the load between sensor nodes is a great challenge for the long run operation of wireless sensor networks [10]. When a sensor node becomes overloaded, the prospect of higher latency, energy loss, and congestion becomes high [11]. The balanced a load cluster head selection aims at decreasing the energy consumption and increasing the network lifetime by introducing load balancing concept in it. If a few cluster nodes are heavily loaded, it leads to faster energy consumption and to get the normal depletion of energy [12]. The balanced load cluster head selection is initiated. The distance between normal child nodes and cluster head plays a major part in energy consumption. So, balanced load cluster head selection leads to nominal energy depletion of each node is presented in the network by creating transmission with closer nodes by a balanced load among the cluster heads.

Algorithm 1: **Balanced Load Cluster Head Selection**	
Step 1	CH advertisement and the counter value are declared as (N/CH)-1 to all CH nodes.
Step 2	CN nodes acknowledgement $\text{DISTANCE}_{(\text{CH})(\text{CN})} = \sqrt{CH_i(x,y) - CN_j(x,y)}$ (1) Where $i = 1,2,3,\ldots\ldots$ 10% of the total nodes, $j = 1,2,3,\ldots\ldots$80% of the total nodes, CH –cluster head, and CN – child node.
Step 3	Eq.1 used to calculate CH and CN distance with $\text{Distance}_{\text{threshold}}$.
Step 4	If$ANCE\ (CH)(CN) < DISTANCEThreshold$, decrement the counter value, else, counter value remains same.
Step 5	If $CV = 0$, Stop comparing
Step 6	If CH reaches CL (capacity limits) rejection information transmission starts.
Step 7	Rejected CN nodes will send the requests to nearby CH node.

3.2.2 Intelligent Based Secured Fuzzy Clustering Algorithm

This algorithm mainly comprises three parameters. They are trust value of nodes, the trust value of the path and the coverage area of the nodes that are sent to the fuzzy-based cluster module to the child nodes [13]. This method concentrates in sub cluster-based routing through using the

Fuzzy S-means (FSM) mechanism and cluster head will be selected randomly and at the initial condition. All the nodes have an equal amount of power [10].

Algorithm 2: **ISFC**

Input –Let N be the set of 30 nodes from WSN
Output – Number of CH
Number of nodes is given, $\epsilon > 0$ indicates tolerance value of matrix A, repeat for j = 1 to N do

Step 1	At the initial stage, random matrix partition occur such that $U_0 \in M_{fc}$
Step 2	Distance formula to obtain distance $D_{ij} = \sqrt{(O_i - N_i)^2 + (O_j - N_j)^2}$, $1 \le i \le c, 1 \le j \le M$ (2)
Step 3	Threshold value computation (Th_o) $R_{in} = \left[\frac{d_i}{E_i}\right]_{i=0}^{n}$ (3) Node N_i identification – node election is random
Step 4	If energy of the all the node is equal then if matrix (N_i) > Th_o, Elect N_i as CH so new matrix will equal matrix (CH), else step 5.
Step 5	if matrix (N_i) < new matrix then elect backup SCH
Step 6	if E > min energy and dist (CH) < SCH so that $Th_1 = [(E_n - \max\{K_i * E_c * t\} * N)/N]$ (4) If matrix (N_i) > $Th_1$and matrix (N_i) will equal new CH and call FSM algorithm and new matrix will equal matrix (CH)
Step 7	Call ACO algorithm for optimal path selection
Step 8	Maintain the routing table with security extension and energy updating.
Step 9	Find the neighbors of each CH
Step 10	Calculate the trust score (TS) and distance of the node (D)
Step 11	Calculate the sum of the distance and trust score for all the nodes
Step 12	Select the node with maximum trust value and minimum total distance.

3.3. Energy Computation

The consumed energy of Child Nodes (CN) and Cluster Head (CH) nodes as well as the total energy consumption of the cluster can be calculated using the following equations:

$$E_{CHnode} = E_{etx} + [N/H - 1]\, E_{erx} + E_{ACK} \quad (5)$$

$$E_{CNode} = E_S + E_{etx} \quad (6)$$

$$E_{SC} = [N/H - 1] * E_{CNode} + E_{CHnode} \quad (7)$$

$$E_{Total} = No\ of\ SCH * E_{SC} \quad (8)$$

$Where: E_{CHnode}$ $is\ the\ energy\ of\ cluster\ head.$

E_{CNode} $is\ the\ energy\ of\ the\ child\ node,$

E_{SC} $is\ the\ energy\ of\ the\ super\ cluster\ head,$

E_{Total} $l\ is\ the\ total\ Energy,$

E_{etx} $is\ the\ transmission\ Energy,$

E_{erx} $is\ the\ receiving\ Energy, and$

E_{ACK} $is\ the\ energy\ for\ ACK.$

According to the distance between the CH nodes and the CN nodes, the transmission power is changed and every sub-clusterhas an equal number of CN nodes [14]. That is given by (N/H)-1. Eachsub-cluster has the initial energy of E_i and the energy spent by the cluster head in each round isE_{CHnode} [1]. Hence lifetime of the network is given as in Equation 5.

$$LT = E_i / E_{CHnode} \quad (9)$$

3.4. Proposed Security Mechanism

The security services in WSN ought to protect the data conveyed over the network and the assets from attacks and bad conduct of nodes. In ESMCHmodel, we sought to achieve the security for the aggregated date in which our security mechanism is based on using Elliptic curve cryptography [15-16].

3.4.1EECC – Enhanced Elliptic Curve Cryptography

Our security mechanism is based on Elliptic Curve Cryptography (ECC) and we modify the origin of ECC to get more security [17]. As shown in Figure 2, the block diagram indicates the process of key generation, encryption, and decryption

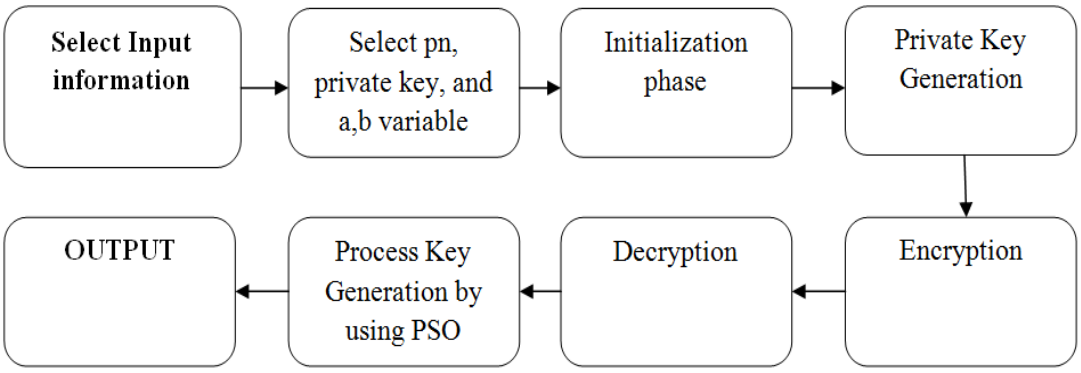

Figure 2- Block Diagram for EECC

3.4.2 Key Generation

The user creates the secret keyKs. Since two keys are created in EECC which is private key (PR_K) and public key (PU_K). The secret key is under gone XOR operation. The best point K_s(k,l) and PU_K is the public key, then the PU_K is given as,$PU_K = PR_K * K_s$

In each transmission round, an encryption key is generated for every SN. The designed encryption key is of 176-bitto overcome the memory constraints of the sensor network [17]. It consists of three components. First component (K_i) is the 148 bits generated by ECC,the second component ($SNID_i$) is the node ID of 13 bits and the third component ($d_{CH,i}$) is the 15 bits for encoding the distance between the CHs and node i. The second component, is allocated 13 bits to make the proposed scheme feasible even in case of large-scale networks that might comprise of thousands of nodes as it allows to represent around eight thousand node IDs [18]. The key at node i is set as $\{K_i, SNID_i, d_{CH,i}\}$.

3.4.3 Algorithm: Plaintext Encryption Process

This algorithm is used to encrypt the date to be more secure so the input and output will be as:

Input: Plaintext represented as S= {a1, a2,….az} .
Output: Ciphertext represented as $\overline{S} = \{\overline{a_1}, \overline{a_2}, \dots \dots \overline{a_Z}\}$

Step 1	Divide the plaintext into Z blocks (size 88 bits), S= {a1, a2,….az} .
Step 2	Generate bit sequence ∂ (size 176 bits)
Step 3	Divide ∂ into equal sized parts, l_1 and l_2 (size 88 bits)
Step 4	Calculate the number of 1's for each byte J [j1, j2,…..,j8]
Step 5	Calculate the number of 1's for each 11 bits K[k1, k2,….,k8] in l_2, For i=1, 2, 3,…., z , calculate these equations: $\mu = l_1 \oplus a_i$ (10) $\bar{\mu} = \text{Permutation}\{\mu, J[i]\}$ (11) $P = \text{concatenation}\{\bar{\mu}, K[i]\}$ (12) $\text{Cipher}[i] = \rho$ (13)
Step 6	Return$\text{Cipher}\ \overline{S} = \{\overline{a_1}, \overline{a_2}, \dots \dots \overline{a_Z}\}$, where $\overline{a_i}$ is the encrypted text of a_i.

3.4.4 Algorithm: Plaintext Decryption Process

For this algorithm, the output from the previous algorithm (Ciphertext) will be the input to get the original data,

Input: Ciphertext represented as $\overline{S} = \{\overline{a_1}, \overline{a_2}, \dots \dots \overline{a_Z}\}$.
Output: Plaintext represented as $S = \{a_1, a_2, \dots \dots a_Z\}$.

Step 1	Receive ciphertext$\overline{S}$ from the CHx
Step 2	Estimate$\lvert N_{count} \rvert$, the number of cluster members
Step 3	Estimate the aggregated data as ∂ = initial $(N * 176)$ bits of $\overline{S}$.
Step 4	Estimate the IDs of cluster members starting from bit index $(N * 176) + 1$ of $\overline{S}$ as $\Psi = \overline{S} - \partial$ (14) $\bar{\partial} = \text{Deaggregate}(\partial)$ (15) $\overline{S}_i = \text{Assign}\{\bar{\partial}, \Psi\}$ (16)
Step 5	Fori $= 1$ to N_{count}do

	– Segment $\bar{S}_i$ into 88-bits blocks $M = \{m_1, m_2, \ldots . . m_{N_{count}}\}$ – Generate bit sequence ϑ (size 176 bits) – Divide ϑ into equal sized parts, l_1 and l_2 (size 88 bits) – Calculate the number of 1's for each byte $J[j_1, j_2, \ldots \ldots j_8]$ – Calculate the number of 1's for each 11 bits $K[k_1, k_2, \ldots . . k_8]$ in l_2
Step 6	Fori $= 1$ to Q calculate these equations $\mu = l_1 \otimes m_j$ (17) $\rho = \text{concatenation}\{\bar{\mu}, K[i]\}$ (18) $\bar{\mu} = \text{Permutation}\{\mu, J[i]\}$ (19) $\text{Plain}[j] = \bar{\mu}$ (20)
Step 7	Return the plaintext$S = \{a_1, a_2, \ldots . . a_Z\}$.

4. RESULT ANALYSIS

4.1. Performance Analysis

The simulation of this proposed model is carried out using the NS2 simulator based on the simulation parameters in Table 1. The proposed model is contrasted with DCSDA [4], ECCDSA [7], and E2HRC [19] by thinking about the overhead, security, accuracy in the data aggregation and energy consumption. Energy consumption is portrayed as the total average amount of energy expected to send and get or forward packets to the destination [20]. Average end to end delay (E2E delay) is characterized as the total time wanted for sending the information to the sink node. The Average Packet Drop ratio is likewise decided as the total average of the dropped packets at the receiving nodes.

Table 1. Simulation Parameters

Parameters	**Values**
Simulation Period	100ms
Coverage Area	1000*1000
No of Nodes	50
No of malicious nodes	5
Cluster Head	1
Sub Cluster	5
Mobile Sink	10
Traffic Type	CBR
Agent Type	UDP
Routing Protocol	AODV
Initial power	100 J
Transmission Power	0.00175 J
Receiving Power	0.00175 J
Queue Type	Drop-Tail

By NS-2 simulator as shown in Figure 3, we can simulate the network of ESMCH model in which child nodes can send the data to Cluster Head (CH) to reach the base station via the Super Cluster Head (SCH).

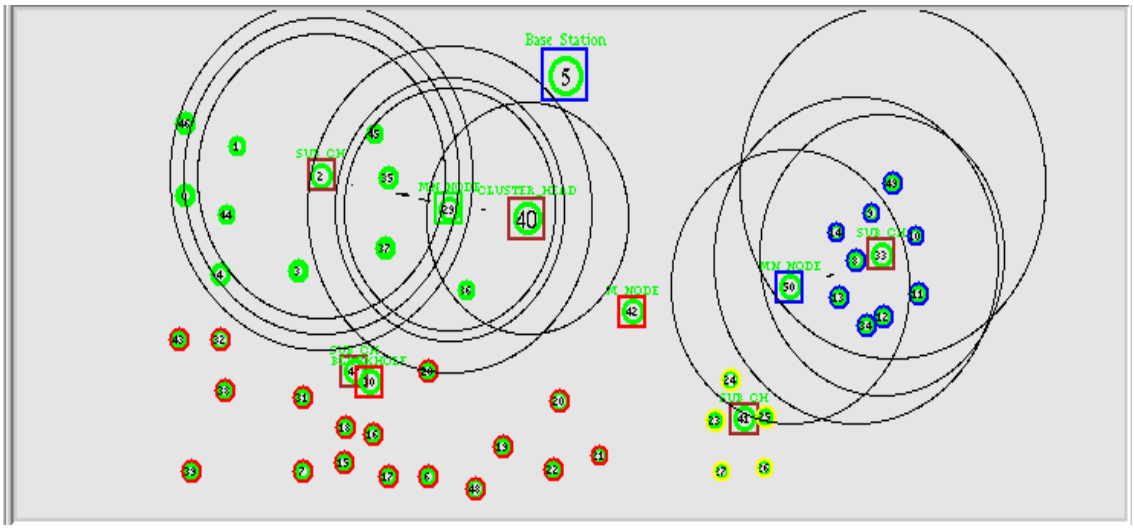

Figure 3: Simulation of the Proposed Model

Figure 4 depicts the packet size ratio compared to network losses. We can achieve that by the ESMCH model; the network is more efficient and has lower losses with the higher value of packet delivery ratio (about 98%) than the compared approaches.

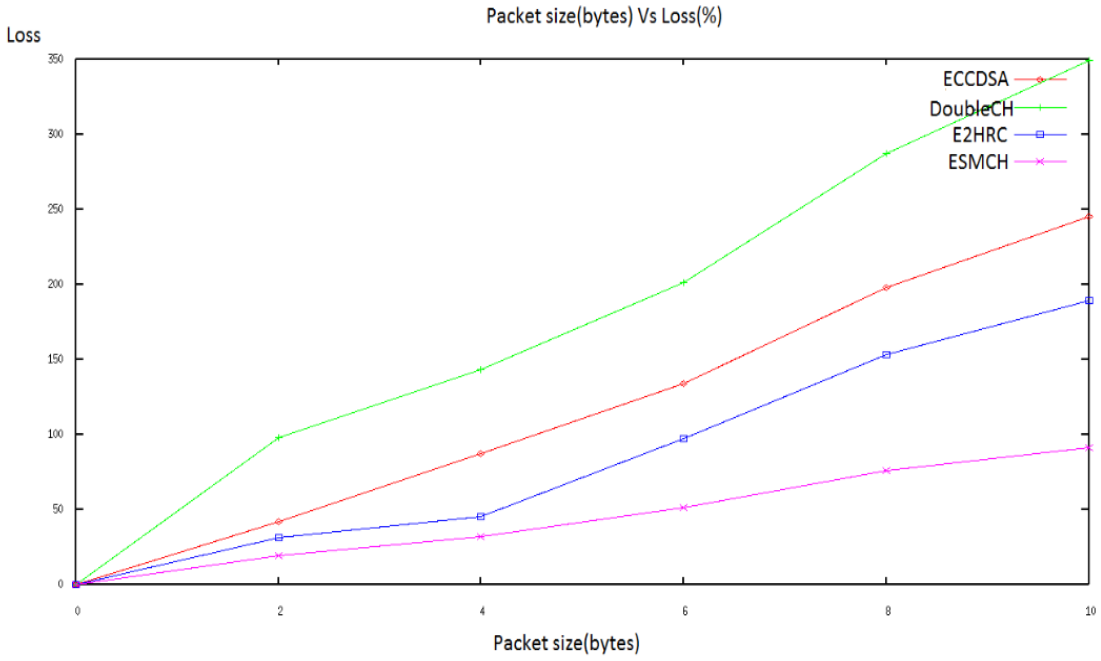

Figure 4: Packet Size versus Losses

Figure 5 shows the total energy consumption of the ESMCH model compared to different models through the network lifetime. ESMCH model has lower energy consumption than the compared approaches. This model can achieve the balancing of the energy consumption between CHs and prolongs the network lifetime.

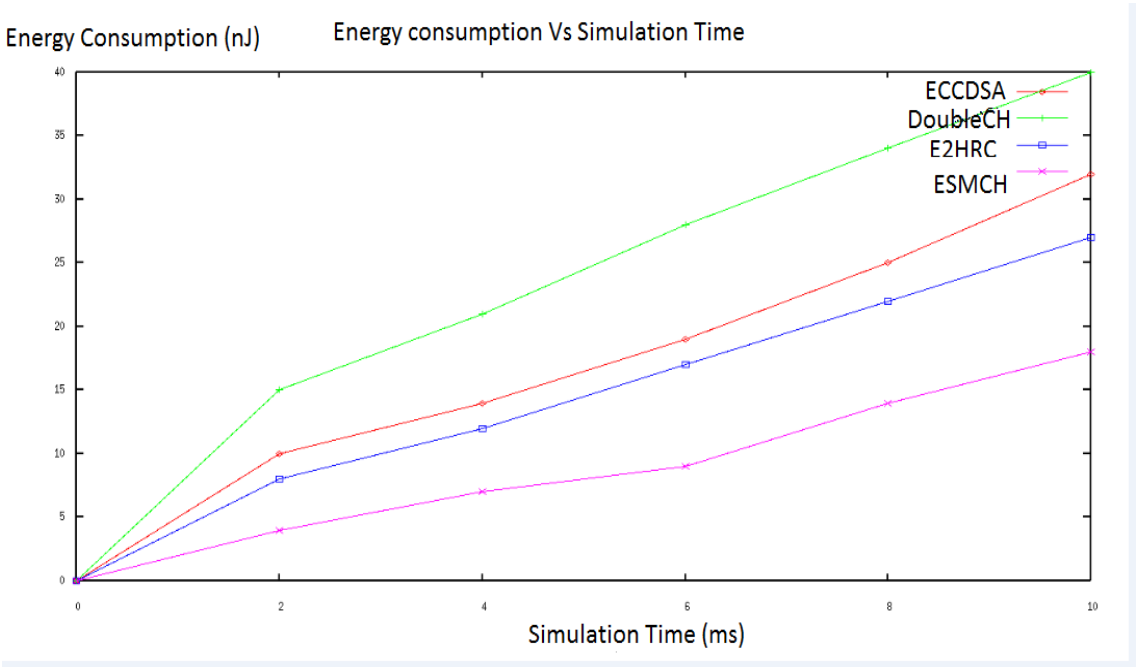

Figure 5: Energy Consumption versus Simulation Time

Routing overhead is known as the ratio of the number of routing-related transmissions. Figure 6 compares the Routing overhead results of ESMCH with some previous approaches in which the proposed model reduces routing overhead.

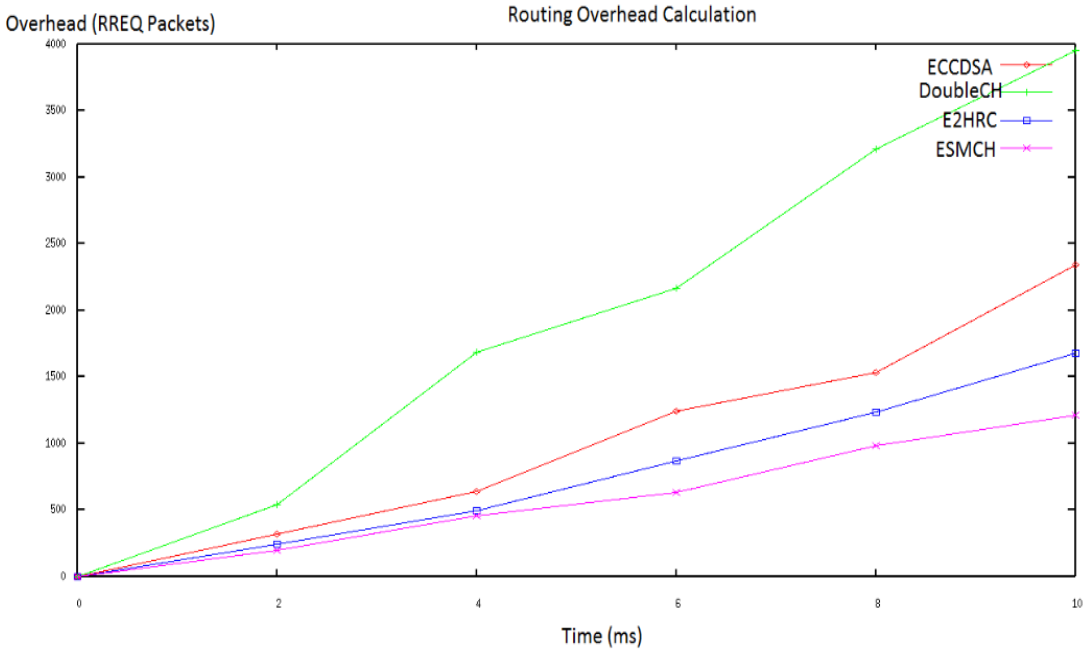

Figure 6: Routing Overhead Calculation of ESMCH

4.2 Security Analysis

In this section, we show that the ESMCH model can stand out some attacks such asMan-in-the-Middle Attack and Black Hole Attack.

a) Man-in-the-Middle Attack: An active foe can change in the transmitted messages between the child nodes and their cluster heads and between cluster heads and super cluster head making them accept that they are communicating with the proposed party. In the ESMCH model, we can encrypt the authenticated information as pursue: private key (PR_K) and open key (PU_K) are generated.$PU_K$is generated as, $PU_K = PR_K * K_s$ to encrypt and send a message (S) with key length of 176-bits which consists of three components {Ki, SNIDi, dCH,i}. We can encrypt and decrypt data using the above algorithms in section 3.4.4.

b) Black hole Attack: an attack is mounted by an external enemy on a subset of the child nodes (CNs) in the network. The enemy captures these nodes then reprograms them so that they can't transmit any data packets. In ESMCH, we can avoid this attack by calculating the distance between neighbour nodes and between cluster head nodes so the list of neighbouring nodes is maintained by each node. The Routing path is made by using AODV Protocol. The generated key is based also in the distance between nodes.

5. CONCLUSION

In this paper, we introduced an efficient and secure malicious node detection model based on a hybrid clustering network for WSNs, which based on the clustering process using one cluster head and mobile trusted nodes. Firstly, the ESMCH model is described with all used algorithms then we analysed the energy computation and security mechanism. The performance is calculated based on delay, packet delivery ratio, drop and throughput. ESMCH model is more secure against some attacks like Man-in-the-Middle Attack and Black hole Attack. By simulation results using NS2 we could prove that the ESMCH model is better in performance and security than these compared models (DCSDA, ECCDSA, and E2HRC) which could help in providing considerable security and reducing energy consumption to increase the network lifetime.

REFERENCES

[1] Kumar, D..Performance analysis of energy efficient clustering protocols for maximising lifetime of wireless sensor networks.IET Wireless Sensor Systems, (2013).

[2] Lee, J. and Kao, T. An Improved Three-Layer Low-Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks.IEEE Internet of Things Journal, 3(6), pp.951-958, (2016).

[3] Neamatollahi, P., Abrishami, S., Naghibzadeh, M., Yaghmaee Moghaddam, M. and Younis, O.. Hierarchical Clustering-Task Scheduling Policy in Cluster-Based Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 14(5), pp.1876-1886,(2018).

[4] A.L.Sreenivasulu, A. and Chenna Reddy, P. Secure Data Aggregation for Wireless Sensor Networks using Double Cluster Head Approach. Journal of Engineering Science and Technology Review, 10(2), pp.75-79 ,(2017).

[5] Trupti Mayee Behara, Umesh Chandra Samal and Sushanta Kumar Mohapatra. Energy-efficient modified LEACH protocol for IoT application. Journal of the Instituation of Engineering and Technology, ISSN 2043-6386,(2017).

[6] Akila, I. and Venkatesan, R. A Fuzzy Based Energy-aware Clustering Architecture for Cooperative Communication in WSN. The Computer Journal, 59(10), pp.1551-1562, (2016).

[7] Tapas Bapu, B. and Siddanna Gowd, L. Security over the Wireless Sensor Network and Node Authentication using ECCDSA. Indian Journal of Science and Technology, 9(39), (2016).

[8] Leu, J., Chiang, T., Yu, M. and Su, K.. Energy Efficient Clustering Scheme for Prolonging the Lifetime of Wireless Sensor Network With Isolated Nodes. IEEE Communications Letters, 19(2), pp.259-262,(2015).
[9] Neamatollahi, P., Abrishami, S., Naghibzadeh, M., Yaghmaee Moghaddam, M. and Younis, O. Hierarchical Clustering-Task Scheduling Policy in Cluster-Based Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 14(5), pp.1876-1886, (2018).
[10] Shanmukhi, M., Nagasatish, G. LOAD BALANCING USING CLUSTERING IN WSN WITH FUZZY LOGIC TECHNIQUES. International Journal of Pure and Applied Mathematics, ISSN: 1314-3395, (2018).
[11] Li, J., Zhou, J. and Zhang, Y. Cluster Head Selection Based on an Information Factor for Wireless Sensor Network Protocol. Journal of Networks, 9(9),(2014).
[12] A, M. and Boukerram, A. Cluster-based Communication Protocol for Load-Balancing in Wireless Sensor Networks. International Journal of Advanced Computer Science and Applications, 3(6).(2012).
[13] Nayak, P. and Vathasavai, B. Energy Efficient Clustering Algorithm for Multi-Hop Wireless Sensor Network Using Type-2 Fuzzy Logic. IEEE Sensors Journal, 17(14), pp.4492-4499, (2017).
[14] ShiouLeu, J., Hung Chiang, T., Chieh Yu, M. and Wu Su, K. Energy Efficient Clustering Scheme for Prolonging the Lifetime of Wireless Sensor Network With Isolated Nodes - IEEE Journals & Magazine. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/6983545, (2014).
[15] Tamer Mohamed Barakat,. An Efficient Secure Key Management Scheme based on Secret Sharing for Hierarchical Wireless Sensor Networks. European Journal of Scientific Research , Vol. 133 No 4, pp.369-385, (2015).
[16] Maleh, Y. and Ezzati, A. A Review of Security Attacks and Intrusion Detection Schemes in Wireless Sensor Network. International Journal of Wireless & Mobile Networks, 5(6), pp.79-90, (2013).
[17] Zargar, A. ENCRYPTION/DECRYPTION USING ELLIPTICAL CURVE CRYPTOGRAPHY. International Journal of Advanced Research in Computer Science, 8(7), pp.48-51, (2017).
[18] Wajgi, D. Load Balancing Based Approach To Improve Lifetime Of Wireless Sensor Network. International Journal of Wireless & Mobile Networks, 4(4), pp.155-167, (2012).
[19] Zhang, W., Li, L., Han, G. and Zhang, L. E2HRC: An Energy-Efficient Heterogeneous Ring Clustering Routing Protocol for Wireless Sensor Networks. IEEE Access, 5, pp.1702-1713, (2017).
[20] Gholamreza, F. Energy Consumption Reduction In Wireless Sensor Network Based on Clustering. International Journal of Computer Networks & communications (IJCNC), Vol.11, No.2, March (2019).