Dynamic CH selection and Intrusion Detection in WSN using Reinforced Weighted Approximation based Adaptive SEECH: An Optimized Routing framework

Sandhya R
Research Scholar, Bharathiyar University, Coimbatore, Tamil Nadu 641046, India.
Orcid: 0000-0003-4298-3685

Sengottaiyan N
Director, Academics Hindustan College of Engineering and Technology, Coimbatore, Tamil Nadu 641032, India.
Orcid: 0000-0002-1949-4771

Abstract:
We propose a highly scalable adaptive cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, we consider multidimensional trust attributes derived from communication and social networks to assess the overall trust of a sensor node. In this paper the Adaptive Scalable Energy Efficient Clustering Hierarchy (Adaptive SEECH) protocol is introduced for the optimized routing with intrusion detection. By means of Dynamic cluster head selection using Harmony Search based Genetic Algorithm (HS-GA), and then the Reinforced Weighted Approximation (RWA) optimization is utilized for our work to balance the trust level and the energy level of the sensor nodes. In this proposed work designing a basic network model with 50 sensor nodes and clustering the nodes by utilizing the algorithm namely Firefly with Nearest Neighbour Chain Clustering algorithm and validate the performance of our proposed routing protocol. The performance analysis and comparison of our proposed routing protocol with some existing routing protocols shows the significance of the proposed work.

Keywords: Adaptive SEECH, Intrusion Detection, Dynamic Cluster Head Selection, Harmony Search based Genetic Algorithm, Reinforced Weighted Approximation, Firefly with Nearest Neighbour Chain Clustering

INTRODUCTION
The recent development in wireless communication technologies have increased the vision of wireless sensor networks (WSN) into reality because of the scalable, low cost, energy efficient sensor architecture [1]. Despite wireless sensor networks have inspired tremendous research interest in diverse application domains such as weather monitoring, traffic monitoring, military, home automation, health care monitoring, security, safety, underwater marine life monitoring, etc. [2]. Wireless Sensor Networks (WSNs) are composed of sensor nodes and sinks which have the capability of self-healing and self-organizing [3]. They are decentralized and distributed in nature where communication takes place via multihop intermediate nodes [4]. The distributed multihop nature of WSN increases the complexity in terms of security attack detection and prevention. In a multihop distributed environment, it is very difficult to locate attackers or malicious nodes [5]. Many security attack detection and prevention mechanisms are designed for WSNs; however most of the existing solutions are capable of handling only a few security attacks [6].

A new media access mechanisms are designed to handle hidden-node problem or selfishness. However there is a need to design mechanisms that are capable enough of detecting and preventing multiple security attacks in WSNs [7]. An Intrusion Detection System (IDS) is one of the possible solution to overcome the security attacks in WSN but cannot prevent or respond to attacks [8]. The IDS may be classified into two types based on rules and anomalies [9]. Rule-based IDSs detect intrusion by matching traffic patterns or resource utilizations. Although anomaly based IDSs have the ability to detect both well-known and new attacks, they have more false positive and false negative alarms. Some IDSs operate in specific scenarios or with particular routing protocols [11].

All the nodes in WSN need some sort of cooperation to detect routing intrusions with the help of proactive routing protocol [12]. The intrusion detection mechanisms operate with reactive routing protocols enable the network to select a reliable path from source to destination [13]. It is essential to select a reliable path with energy efficient node for transmission which remains a challenging issue in WSN. Therefore, the protocols that are designed to work with
Intrusion detection in WSNs should consider energy efficiency as a primary goal [14]. There is much attention on energy efficiency of clustering protocols designed around cluster based network structure [15]. The clustering approaches can increase network longevity and improve energy efficiency by minimizing overall energy consumption and balancing energy consumption among the nodes during the network life time [16].

The clustering based protocols are classified with respect to the techniques they adopt to select cluster heads and transmitting the aggregated data to the data sink [17]. In order to transmit aggregated data to the data sink the protocols use either single-hop communication or multihop communication which may cause energy unbalancing [18]. The LEACH protocol assumes that energy consumption is equal in nodes when they are selected as cluster heads and/or non-cluster head [19]. The TL-LEACH uses two cluster head layers to reduce intra-cluster communication energy consumption [20]. The EECS protocol gives a fair distribution for cluster heads [21]. The HEED protocol selects the cluster heads based on residual energy and the minimum power level required by a node to communication with its cluster head, and the cluster head send the data to data sink using a multi-hop communication approach [22]. The TCAC protocol selects the cluster head same as the EECS protocol while tries to balance size of clusters, and the cluster head nodes send the data to the data sink directly [23]. However the performance of these conventional protocols get degraded because of inappropriate cluster head selection, high energy consumption of transmitter and receiver and the distance between the data sink and network. Such behaviour makes these clustering techniques inefficient from an energy efficiency perspective [24].

In order to overcome the above issues in this research work we contribute to design a novel hierarchical routing protocol named as Adaptive Scalable Energy Efficient Clustering Hierarchy (Adaptive SEECH) protocol with trust management using Reinforced Weighted Approximation Algorithm (RWAA) for Intrusion detection. In addition to that we also contribute to design Harmony Search based Genetic Algorithm (HS-GA) for dynamic cluster head selection from the clusters formed by Firefly based Nearest Neighbour Chain (FNNC) Algorithm. The remainder of this article is organised as follows: Section 2 presents an overview of some of the recent works very related to our proposed research work. Section 3 briefs the design of the proposed routing protocol. Section 4 presents the simulation results of the proposed work with performance analysis followed by the conclusion in section 5.

**RELATED WORK**

Some of the very recent works related to routing in wireless sensor network based on clustering hierarchy is listed below:-

Mehdi Tarhaniet.al [25] have proposed a new distributed algorithm named Scalable Energy Efficient Clustering Hierarchy (SEECH), which selects CHs and relays separately and based on nodes eligibilities. In that way, high and low degree nodes are, respectively, employed as CHs and relays. Although, CHs and relays are different, but their goal was mainly mitigation of CHs energy burden which is intrinsically satisfied by the new distributed algorithm. To consider uniformity of CHs to balance clusters, SEECH used a new distance-based algorithm. To evaluate the scalability of SEECH strategy, simulations were conducted in three different network size scenarios. FenyeBaoet.al [26] have proposed a highly scalable cluster-based hierarchical trust management protocol for Wireless Sensor Networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, they considered multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a probability model, they described a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviours with the objective to yield “ground truth” node status. This served as a basis for validating the protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of the hierarchical trust management protocol, they applied it to trust-based geographic routing and trust-based intrusion detection.

Hamid Al-Hamadi and Ing-Ray Chen [27] have proposed redundancy management of Heterogeneous Wireless Sensor Networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of redundancy management was to exploit the trade off between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. They formulated the trade off as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability was maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm was applied to detect and evict malicious nodes in a HWSN. They developed a novel probability model to analyse the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN was maximized.

NoureddineLaslaet.al [28] have proposed a secure routing protocol named Secure Multi-paths Routing for wireless sensor networks (SMART) as well as its underlying key management scheme named Extended two-hop Keys
Establishment (ETKE). The introduced framework keeps consistent routing topology by protecting the hop count information from being forged. It also ensured a fast detection of inconsistent routing information without referring to the sink node. They analysed the security of the proposed scheme as well as its resilience probability against the forged hop count attack. They have demonstrated through simulations that SMART outperformed a comparative solution in terms of energy consumption.

Qi Guo et al. [29] have proposed a universal method: MP-ID (Multi-Protocol Oriented Middleware-level Intrusion Detection) to solve the problem of multi-protocol intrusion detection. MP-MID can generate all known attack types for any routing protocol of WSN, and furthermore, all of them can be detected with the automatically generated rules. They formalized the routing protocol with the Process Algebra for Wireless Mesh Networks (AWN) language, and proposed the conception of attack points to find out all attack types. Combining attack points with formalized protocol in AWN, result in co-sentences which represent the attack features in the protocol. With program slicing technology, all known attack types can be found out based on co-sentences. According to the characteristic of the key variables of the attack types, MP-MID can generate misuse based detection or anomaly based detection.

Shahaboddin Shamsirband et al. [30] have proposed an ahybrid clustering method namely a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA). Hereby, the Imperialist Competitive Algorithm (ICA) was modified with a density-based algorithm and fuzzy logic for optimum clustering in WSNs. A density-based clustering algorithm helps to improve the imperialist competitive algorithm for the formation of arbitrary cluster shapes as well as handling noise. The Fuzzy Logic Controller (FLC) assimilates to imperialistic competition by adjusting the fuzzy rules to avoid possible errors of the worst imperialist action selection strategy.

Optimized Routing by Adaptive Speech

Wireless environments give more design challenges due to the presence of large number of small sensor nodes, which are provide inherently unreliable communication. Also sometimes the nodes may compromised and perform malicious attacks to disturb the normal operation of a wireless network. Generally known that the sensor nodes in WSNs are energy limited, thus leading to limited communication range, weak processing capacity and restricted storage space on each sensor node. This ultimately makes WSNs vulnerable to intrusions such as packet dropping or packet modifications to disrupt normal operations of a WSN wherein SNs usually perform unattended operations. The traditional cluster-based communication protocols such as LEACH, SEECH play a considerable role for energy saving in hierarchical wireless sensor networks. In such protocols a cluster head (CH) simultaneously serves as a relay sensor node to transmit its cluster/other clusters data packet(s) to the data sink. As a result, each node would have CH role as many as relay role during network lifetime. Such behaviour makes these clustering techniques inefficient from an energy efficiency perspective. So that WSN with large number of sensor nodes require a scalable algorithm for highly reconfigurable communication operations. In this research work we propose to design an Adaptive SEECH protocol with dynamic cluster head selection and Intrusion detection strategy. The architecture of our proposed routing framework is shown in figure 1.

Initially the sensor nodes of WSN are clustered using FNNC. Initially the sensor nodes of WSN are clustered using FNNC algorithm and the energy level as well as the trust level of each node is calculated by forwarding a sample packet through the nodes. From the result of trust metric the intruded nodes are detected, in addition to that the optimal energy efficient cluster heads is also selected from each cluster based on the trust metric and energy level simultaneously. The dynamic cluster head selection is performed by the utilization of Harmony search based genetic algorithm. And finally the optimal path for data forwarding is selected and the introduction of RWAA before data forwarding optimizes the trust level of the nodes to reduce the energy consumption.

System Model

To analyse the performance of our proposed routing protocol it is essential to define the system model with the corresponding expectations and assumptions. In this research work we assume a wireless sensor network with \( N \) number of sensor nodes and a sink node which are randomly distributed without mobility. Such network can be modelled as a graph given by:

\[
G_{\text{WSN}} = (N, L) \tag{1}
\]

Where \( G_{\text{WSN}} \) is a unit disk graph. \( N \) is the set of sensor nodes, and \( L \subseteq N \) is the set of links among the nodes. Also we
consider the following assumptions in the network model.

- All the sensor nodes have the same transmission ranges which are represented by a unique identifier ID.
- The communication pattern is many-to-one between sensor nodes and the sink node.
- The data sink is located far from the sensing field. Sensor nodes and data sink are all stationary after deployment.
- Sensor nodes are location-unaware that means they are not equipped with GPS or other similar equipment.
- Periodically the recently sensed data and information by all nodes are gathered and sent to the data sink after aggregation.
- Nodes have the same capabilities and resources. Each sensor node is assigned a unique identifier (ID).
- Nodes are capable of acting in inactive mode or a low power sleeping mode.
- Sensors can control power level to adjust the amount of transmission power according to the distance to the desired recipient.
- The links are assumed to be symmetric. A node can estimate the distance to another node based on the received signal.

Routing Via Adaptive SEECH (ASEECH)

The proposed ASEECH routing protocol starts with the number of nodes in the network area which are distributed randomly. Then the nodes are grouped in order to from a number of clusters in the network by the utilization of Firefly based Nearest Neighbour Chain (FNCC) Algorithm. In our FNCC algorithm the location of each node is taken into consideration so that costly intra-cluster communications could be avoided.

Firefly based Nearest Neighbour Chain Algorithm

The process of clustering is a primary metric for evaluating the performance of a sensor network and it has been shown to improve network lifetime. Many clustering algorithms specifically designed for WSNs for scalability and efficient communication. In particular, WSNs are conveyed in an ad hoc manner and have a large number of nodes. The nodes are typically unaware of their locations. Consequently, distributed clustering protocols that rely only on neighbourhood information are preferred for WSNs. In our proposed work the firefly based nearest neighbour chain algorithm is utilized for efficient clustering of the nodes in WSNs.

In the firefly algorithm there are two important considerations such as attractiveness and distance. A firefly’s attractiveness is considered as similarity of the nodes present in the proposed network model. In order to determine the distance between the nodes we propose to calculate the Cartesian distance of the nodes. In the phase of distance calculation we integrate the Nearest Neighbour Chain algorithm with the firefly algorithm which helps to find the centre of the clusters with the most optimal neighbour nodes present in the network. The attractiveness of the firefly can be expressed as:

$$\beta(r) = \beta_0 e^{-r^2}$$  \hspace{1cm} (2)

where $\beta_0$ is the attractiveness at $r = 0$ and $\gamma$ is the light absorption coefficient, value of $\gamma$ is taken as 1. The Cartesian distance between any two sensor nodes can be calculated by:

$$D(x, y) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$  \hspace{1cm} (3)

Where $x, y$ denotes the different nodes present in the network, $i$ and $j$ denotes the different location of the nodes present in the network. The movement of the firefly $i$, which is attracted to another more attractive firefly $j$ is determined by:

$$X_i = x_j + \beta_0 e^{-r^2} (x_j - x_i) + \alpha (rand - 0.5)$$  \hspace{1cm} (4)

In order to find the center of the clusters with the proposed FNNC algorithm the objective function can be formulated as follows:

$$Objective\ function = Dis(X,Y) = \sqrt{\sum_{i=1}^{n} (X_{pi} - Y_{pi})^2}$$  \hspace{1cm} (5)

Where $X_{pi}$ is the $p^{th}$ data path vector and $Y_{pi}$ is the distance vector of cluster $j$. It is essential to determine the minimum value of the objective function until the iteration stopped. After the each iteration the distance and the movement of the firefly should be updated. The updation of the distance can be expressed by:

$$D(x_{best}, y_{best}) = \sqrt{(x_i - x_{gbest})^2 + (y_i - y_{gbest})^2}$$  \hspace{1cm} (6)

And the updation of firefly movement can be expressed as:

$$X_{best} = x_i + \beta_0 e^{-r^2} (x_j - x_i) + \beta_0 e^{-r^2} (x_{gbest} - x_i) + \alpha (rand - 0.5)$$  \hspace{1cm} (7)

From the below clustering algorithm the term fireflies are consider as nodes for the proposed work. The parameters current best and global best constitutes of the current best location of the node (i.e this current best of the particular node is better than the previous location) and the optimal location in WSN respectively. Here the global best constitutes the centroid of the cluster. The steps in the proposed clustering algorithm can be explained as follows:
Begin
Initialize fireflies with random population \( K \) and number of cluster centres \( D \).
Define the light absorption coefficient \( \gamma \). \( (\gamma = 1) \)
If \([t<\text{max(iteration)}]\)
Calculate the objective function using equation (7).
If \((ij>i)\)
Move firefly \( i \) toward \( j \) based on equation (9) to update the locations.
End if
End if
Find the current best and global best values of the fireflies.
Initialize the centre of the cluster by global best.
Update the cluster location
Stop until the maximum iteration reached.
End

Algorithm 1: Steps in FNNC Algorithm

The clusters resulted from the FNNC algorithm might disturbed by several attacks in the network. So as to detect such nodes disturbed by the attacks (Intrusion) we forward a sample data through the nodes and determine the energy level and trust level of the nodes.

Intrusion detection
An intrusion is basically any sort of unlawful activity which is carried out by attackers to harm network resources or sensor nodes. Intrusion detection (ID) is a mechanism to detect such unlawful or malicious activities. The primary functions of ID are to monitor users/ nodes’ activities and network behaviour at different layers. With the intention of intrusion detection of network in the proposed work we calculate the energy metric as well as the trust metric of each node after forwarding the sample data through it.

Energy Metric
To generate a node energy model that can precisely reveal the energy consumption of sensor nodes is an extremely important part of protocol development, system design and performance evaluation in WSNs. Energy is one of the most important resources in WSNs and the energy is needed to transmit, receive and deal with sensory data. In this work we assume that each sensor node has the same initial available energy level, while the sink node has high power and calculation capacity than the sensor node. The energy consumed by a sensor node while transmitting a \( k \) bit message over a distance \( d \), is given by:

\[
E_T(k,d) = E_{T-elec}(k) + E_{T-amp}(k,d) = \begin{cases} 
ke_{elec} + ke_{fs}d^2, & d < d_0 \\
ke_{elec} + ke_{mp}d^4, & d > d_0 
\end{cases} \tag{8}
\]

Similarly the energy consumption of a node while receiving the \( k \) bit message can be calculated by:

\[
E_R(k,d) = kE_{elec} \tag{9}
\]

Where \( E_{elec} \) is the Electronics energy which can be resulted from the signal processing techniques such as modulation, filtering and digital coding. \( e_{mp}d^4 \) or \( e_{fs}d^2 \) is the amplifier energy which depends on the distance to the receiver and the acceptable Bit Error Rate (BER). And the upcoming section describes the proposed routing protocol.

Trust metric:
A trust model is required to find malicious, selfish and compromised insiders by evaluating trust worthiness sensors from the network. It improves the lifetime of networks that inspire expectations among future interactions of the sensor nodes. In our proposed work we compose our trust metric by considering both social trust and QoS trust to take into account the effect of both aspects of trust on trustworthiness. Social trust in the context of wireless sensor nodes (SN) may include intimacy, honesty, healthiness, unselfishness. QoS trust may include energy, connectivity. The overall trust metric of a sensor node can be calculated as

\[
T(SN) = T_{social}(SN) + T_{QOS}(SN) \tag{10}
\]

Where

\[
T_{social}(SN) = w_1T_{intimacy}(SN) + w_2T_{honesty}(SN) + w_3T_{healthiness}(SN) + w_4T_{unselfishness}(SN) \tag{11}
\]

\[
T_{QOS}(SN) = w_5T_{energy}(SN) + w_6T_{connectivity}(SN) \tag{12}
\]

\[
w_1 + w_2 + w_3 + w_4 + w_5 + w_6 = 1 \tag{13}
\]

\( w_1, w_2, w_3, w_4, w_5 \) and \( w_6 \) are the weight vectors.
Healthiness: When a node $i$ meets node $j$ they will share the encountered history of them to each other. If node $j$ is malicious, then the shared history between the two sensor nodes is inconsistent. There results the trust metric equal to zero. The healthiness trust calculation can be expressed as:

$$T_{healthiness}(SN'_i) = \begin{cases} 
1, & \text{if } EH(i) = EH(j) \\
0, & \text{otherwise}
\end{cases}$$

(14)

where $EH(i)$ is the encountered history matrix of $i$, $EH(j)$ is the encountered history matrix of $j$. The encountered history matrix can be represented as:

$$EH(i) = \begin{bmatrix} j \rightarrow (3), ENC_{ij}' \\ k \rightarrow (2), ENC_{jk}' \end{bmatrix}$$

(15)

From the above matrix it is shown that node $i$ encounters $j$ three times, node $k$ two times.

Unselfishness: This provides the degree of unselfishness of node $j$ as evaluated by node $i$ based on direct observations over $[0, t]$. This can be calculated by marinating a friend list in each of the nodes where the corresponding node also included itself as a member in the friend list. If node $i$ is considered as a source node and node $j$ is the destination with node $k$ as an intermediate node the unselfishness trust can be calculated as follows:

$$T_{unselfishness}(SN'_i) = \begin{cases} 
T + 10, & \text{if } i \text{ or } j \in FL(k) \\
0, & \text{otherwise}
\end{cases}$$

(16)

Intimacy: This measure the level of interaction experiences following the trained model. It is computed by the number of interactions between nodes $i$ and $j$ over the maximum number of interactions between node $i$ and any neighbour node over the time period $[0, t]$.

Honesty: This refers to the belief of node $i$ that node $j$ is honest based on node $i$’s direct observations toward node $j$. Node $i$ estimates $T_{honesty}(SN'_i)$ by keeping a count of suspicious dishonest experiences of node $j$ which node $i$ has observed during $[0, t]$ using a set of intrusion detection rules. If the count exceeds a system-defined threshold, node $j$ is considered totally dishonest at time $t$, which can be expressed as:

$$T_{honesty}(SN'_i) = \begin{cases} 
0, & \text{if } N > T \\
1 - \frac{N}{T}, & \text{otherwise}
\end{cases}$$

(17)

where $N$ is the hop count. $T$ is the fixed threshold. The compromised node must be dishonest.

Energy: This refers to the belief of node $i$ that node $j$ still has adequate energy to perform its intended function. The energy trust can be calculated from the following expression when a node $i$ sends a packet to node $j$ through node $k$:

$$T_{energy}(SN'_i) = \frac{ack(i \rightarrow j)}{P(i \rightarrow j)}, \text{via node } k$$

(18)

Where $P(i \rightarrow j)$ represents the number of packets transmitted from node $i$ to node $j$ via node $k$.

Connectivity: When the node $j$ with $i$ found connectivity in the network during sample packet transmission the connectivity between node $i$ and node $j$ can be expressed as:

$$T_{connectivity}(SN'_i) = \frac{Enc(i \rightarrow j)}{Enc(n \rightarrow j)}$$

(19)

Where $n$ represents any node in the network, $Enc(i \rightarrow j)$ represents the number of encounters between node $i$ and node $j$. The trust value obtained for each node using equation (10) is now normalised to the scale of ‘0’ to ‘2’ using the expression given as:

$$T(SN)_{norm} = 2 \left[ \frac{T(SN)}{T_{max}} \right]$$

(20)

where $T_i$ is the trust level of the node $i$. Maximum trust level obtained. From the $T(SN)_{norm}$ value the malicious nodes can be identified using the below table 1.

<table>
<thead>
<tr>
<th>Trust level $T(SN)_{norm}$</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&lt;1$</td>
<td>Malicious nodes</td>
</tr>
<tr>
<td>$&gt;1$</td>
<td>Good nodes</td>
</tr>
</tbody>
</table>

From table 1 we can classify the good nodes and malicious nodes present in the network. A SN is more likely to become malicious when it has low energy or it has many unselfish neighbour nodes around. Further, a SN is more likely to become compromised when it has more compromised neighbours around.
**Dynamic CH selection by Harmony search based Genetic Algorithm**

Instead of each node sending their own data directly to the base station, nodes in a cluster send their data to the cluster head, then the cluster head aggregates the received data and send it to the base station. During the set-up phase, each node sends information about its current location and residual energy level to the sink. Sink computes the average node energy, and determines which nodes have energy below this average. Selection of CH is challenging because of the locations of the nodes in the network. Several LEACH based algorithms were proposed in the last decades for the process of CH selection. However, the traditional algorithm doesn’t consider the position of the nodes in cluster-head selection. Therefore a node in the boundaries of a cluster might be elected as CH. This decision drains the energy of the network due to the higher distance between the nodes. The CH Optimized selection of cluster heads is an NP-Hard problem, we utilize a Genetic Algorithm based Harmony Search (GA-HS) Algorithm for optimal cluster head selection.

In the proposed GA-HS optimization initially the number of node in the network are assumed to be the initial population. Once the population is initialized or an offspring population is created, the fitness values of the candidate solutions are evaluated by the expression given as:

\[ F(x) = \max \left[ \frac{T(SN)}{E(SN)} \right] \]  \hspace{1cm} (21)

Where \( E(SN) = E_r(SN) + E_k(SN) \), \( E(SN) \) is the energy consumed by each node, \( T(SN) \) is the trust level calculated from each node. Then the Selection process allocates more copies of solutions with higher fitness values and thus imposes the survival-of-the-fittest mechanism on the candidate solutions. The crossover process combines the parts of two or more parental solutions to create new, possibly better solutions which can be given by:

\[ X^i_j = [\text{uniform}(0,1)]x^i_j + [1-\text{uniform}(0,1)]x^i_{rand} \]  \hspace{1cm} (22)

Then the mutation performs a random walk in the neighbourhood of a candidate solution which can be given by:

\[ x^*_{k_i} = x_{k_i} + \text{rand} \times N(0,1) \]  \hspace{1cm} (23)

Then the worst fitness solution is updated using the HS operators which are given by:

\[ x^\text{new}_{\text{worst}} = x^\text{old}_{\text{worst}} + v^\text{new}_{\text{worst}} \]  \hspace{1cm} (24)

where \( v^\text{new}_{\text{worst}} \) is the updated position of the nodes. All the above process performed in GA-HS can be simply explained by the following algorithm.

**Algorithm 2: Cluster head Selection by GA-HS**

The GA-HS results the optimal node from each cluster as CH which consume low energy with high trust level. Thus the dynamic selection of CH, which is capable of transferring the information received from the other nodes to the base station in an efficient manner to increase the energy efficient with the trust level.

**Optimized trust management**

When the system senses that the hostility expressed in terms of the percentage of compromised or malicious nodes is increasing, it can dynamically adjust \( T_{social} \) to optimize the performance in terms of message delivery ratio. In this research work the dynamic trust management can be done by Reinforced Weighted Approximation (RWA) algorithm which aims to balance the trust level and the energy level of the nodes which are presented in the boundary of the clusters.

The objective function for the RWA optimization can be defined as:

\[ F(x) = T_{QoS} + \lambda T_{social} = T(CH) \]  \hspace{1cm} (25)

Where \( \lambda \) is the optimizing parameter used to adjust the value of \( T_{social} \). The proposed Reinforced Weighted Approximation Algorithm automatically learns the trust value of the sensor node \( T(CH) \) and adjust the parameter \( \lambda \) to maintain the condition expressed in (25). The processing step of RWA can
be simply explained by the following.

Initialize the number of nodes, $\lambda$ and the trust level calculated for each node.
Set the fixed value for $T(CH)$.
For ($t< maximum$ iteration)
Evaluate the fitness function using (25).
Update the value of $\lambda$ and find the optimal best value.
Replace $\lambda$ by the optimal best value.
Repeat until the maximum iteration reached.

Algorithm 3: Optimal trust management by RWA

From the result obtained by the RWA optimization the trust value of the sensor nodes and the cluster heads will be maintained at a stable level. From the cluster heads selected by the above process only the efficient CHs placed which are present at the shortest distance from the source to destination is chosen and the original data will be forwarded through it.

Protection of internal attacks
The selective forwarding attack is described as when the parts of packets are dropped in the place of compromised nodes which is important to forward. This attack is the major concern in the wireless sensor networks. If a compromised node discards all the packets, it is defined as black hole attack. In view of the interaction of nodes, utilizing our trust assessment system could effectively defend both the selective forwarding attack and black hole attack. Briefly, the trust value of these compromised nodes will continue to decrease with time going. Slander attack is defined as the action that a compromised node transfers the unfair deny evaluation of normal node to decrease its reputation. A compromised node can also work like a normal node and cumulate high enough reputation in order to provide trust evaluation error for other compromised nodes, which is defined as collusion attack.

Generally known that the sensor nodes in WSNs are energy limited, thus leading to limited communication range, weak processing capacity and restricted storage space on each sensor node. This ultimately makes WSNs vulnerable to intrusions such as packet dropping or packet modifications to disrupt normal operations of a WSN wherein SNs usually perform unattended operations. Thus the research work discuss the efficient clustering and dynamic CH selection to design an energy efficient routing protocol with intrusion detection in WSN, which is very essential to balance energy consumption and prolong network lifetime with high trust level.

SIMULATION RESULTS

The simulation setup of our proposed methodology, the obtained results, its performance evaluation and the discussion of its efficiency compared to the existing protocols are presented in this section.

Simulation setup
The proposed routing framework is implemented in the MATLAB platform of version R2013a with the system configurations of Intel i5 processor embedded in the personal computer operating at the speed of 2.99 GHz with memory storage of 8GB RAM in Windows 8 (64 bit) Operating System. The simulation parameters used in the proposed work was given in table 1.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{elec}$</td>
<td>0.5</td>
</tr>
<tr>
<td>$d_0$</td>
<td>1 m</td>
</tr>
<tr>
<td>$\varepsilon_{mp}$</td>
<td>0.0013PJ/bit/m$^2$</td>
</tr>
<tr>
<td>$\varepsilon_f$</td>
<td>10 PJ/bit/m$^2$</td>
</tr>
<tr>
<td>$T$</td>
<td>20</td>
</tr>
<tr>
<td>$r$</td>
<td>0.35m</td>
</tr>
</tbody>
</table>

The WSN is initially assumed with having 50 nodes, each of them with a Transmission range of 85 m and they are arranged into the virtual topology using FNNC algorithm and each of the clusters has N number of nodes. Within the Clustering framework the sample packet Transmission is initiated by sending 100 packets with each packet having a size of 20 bytes, encrypted with the secret key. The Trust Level parameters are measured at the interval of $(t, t + \Delta t)$. The type of nodes present in the network is initially assumed as given in the following table 2.

<table>
<thead>
<tr>
<th>Nature of Nodes</th>
<th>Number of Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well Behaved Nodes (WB)</td>
<td>40</td>
</tr>
<tr>
<td>Malicious Nodes (MN)</td>
<td>10</td>
</tr>
<tr>
<td>Total number of nodes</td>
<td>50</td>
</tr>
</tbody>
</table>

After transmitting the number of sample packet transmission in the network then the energy level and trust level for each node is calculated to detect the intrusion detection in the
network. The result of our proposed method is discussed in the upcoming section.

RESULTS OF PROPOSED METHOD

In proposed method the WSN is assumed with the 50 number of nodes, then by utilizing FNNC algorithm clustering the number of nodes in the WSN according with the distance calculation with centre of the clusters and optimal nodes. In our proposed method the number of cluster is 3 and for the first, second, third cluster has the number of sensor node is 20, 20, 10 respectively. The malicious nodes are detected according with the both energy level and trust level of the nodes in each cluster. The following figure 2 shows the transmitted energy with different nodes density as 25, 50, 75 and 100. The energy level consumption of the sensor nodes for the proposed is low without malicious nodes compared to WSN with malicious nodes

As a result the above figure 3 shows the comparison of cluster head selection with malicious node and without malicious nodes for the nodes density as 25,50,75 and 100. The performance evaluation of the proposed method is discussed in the following section.

Performance Evaluation

The performance of our proposed secure Trust Level based routing with node categorization are analysed in terms of different parameters such as Trust Level calculated for every node in the network, Packet Delivery Ratio and Throughput. The results are tabulated as well as illustrated graphically.

Packet Delivery Ratio (PDR)

The Packet Delivery Ratio is the metric used to measure the delivery level of the routing Protocol. This measure can be calculated using the equation (26).

$$ D_p = \frac{\sum_{t=1}^{T} \sum_{n=1}^{N} R_{P_{tn}}}{\sum_{t=1}^{T} \sum_{n=1}^{N} S_{P_{tn}}} $$

Where, $R_{P_{tn}}$ = Number of packets received at the nodes in the network over the time T  
$S_{P_{tn}}$ = Number of packets sent through the nodes in the network over the time T

End to End Delay

The End to End Delay is the measure of the average time taken by the data packets to reach their destinations. This delay also includes the time associated with the route finding process and the parameter is only measured in the case where the packets successfully reached their destinations. The End to End Delay for the data packets is calculated using the equation (27).

$$ d_{end-end} = \frac{\sum_{n=1}^{N} (T_A - T_S)}{\sum_{n=1}^{N} N_C} $$

Where, $T_A$ = Arrival time of data packets, $T_S$ = Sending time of data packets, $N_C$ = Total number of connections formed in the network

Figure 2: Energy consumption level

The cluster head selection for each cluster with the objective of low level energy consumption with high trust level of sensor nodes. Before selecting the CH, detect the malicious nodes of the WSN with the help of trust level and energy level.

Figure 3: Cluster head selection Vs Time
**Throughput**

Throughput is the measure of the number of packets transmitted over the network per unit of time. This is usually measured in bits per second (bps) and calculated using the equation (28).

\[
Throughput = \frac{\sum (P_t)}{T}
\]  

(28)

Where, \( P_t \) = Number of packets transmitted, \( T \) = Time measured in seconds.

**Comparative analysis**

The comparative analysis is discussed between the existing and the proposed method by the routing protocols such as Adhoc On Demand Distance Vector Routing Protocol (AODV), Destination sequenced distance vector (DSDV), Dynamic Source Routing (DSR) and proposed routing protocol as ASEECH. The proposed method shows better results than the existing methods in terms of parameter evaluation and the each parameter gives the better results than the existing approaches. Figure 4-6 shows the graphical representation of comparison between our proposed methods with some existing approaches based on the computed values.

**Figure 4: PDR analysis**

The Figure 4 shows the comparison of packet delivery ratio of proposed and existing protocols. This metrics illustrates the level of delivered data to the destination and the parameter is measured in terms of percentage. The greater the value of packet delivery ratio means the better performance of protocol. Here also overall performance of ASEECH Protocols is better than AODV, DSDV and DSR. So highest the packet delivery ratio greater it has the ability to send packet more to various nodes.

**Figure 5: Analysis of Throughput**

The figure 5 shows the analysis of throughput of proposed protocol with three existing protocols. The overall throughput of ASEECH is better than existing protocols and it is measured in terms of kilobits per second (kbps).

**Figure 6: Comparison of end to end delay**

The figure 6 shows the comparison of the end to end delay between existing and proposed method and ASEECH protocol is better than the other existing protocol.

**DISCUSSIONS**

The hierarchical routing protocol named as Adaptive Scalable Energy Efficient Clustering Hierarchy (Adaptive SEECH) protocol with trust management using Reinforced Weighted Approximation Algorithm (RWAA) for Intrusion detection is proposed in this paper. The existing researches included are...
AODV, DSDV and DSR which is the viable routing protocols for the reliability of wireless sensor networks in the past decades. When we compare our implemented research and the previous routing strategies in the literature the proposed framework has the better result. The above execution assessment and comparison figure 4-6 shows that our proposed technique is superior to the existing strategies in terms of Throughput, packet delivery ratio and end to end delay. Thus the proposed method works quicker than different existing methods. So we can say our proposed method produces the energy efficient routing is very precise and effective.

CONCLUSION

In this research work the adaptive cluster-based hierarchical trust management protocol is introduced in the wireless sensor network. The Nearest Neighbour Chain algorithm with the firefly algorithm which helps to find the centre of the clusters with the most optimal neighbour nodes present in the network. For the intrusion detection of a WSN trust level and the energy levels are computed and also increase the life time for the highly trust level nodes. An efficient Dynamic cluster head selection using genetic algorithm based harmony search algorithm is utilized for the cluster head selection with optimal route selection. The performance evaluation of the proposed method is done in behalf of the metrics such as throughput, packet delivery ratio and end to end delay. From the results and comparison it was observed that our proposed method is technically viable option among the available other routing protocols algorithms.

REFERENCES


