RESOURCEFUL AND SECURE ROUTING PROTOCOL VIA ACTIVE HIERARCHICAL CLUSTERING MECHANISMS FOR WIRELESS SENSOR NETWORK

SASIKUMAR M[1], Dr. R. ANITHA[2]
[1]Assistant Professor, Dept. of Applied Mathematics and Computational Sciences, PSG College of Technology, Coimbatore, Tamilnadu, India.
[2]Director cum Head, Dept. of Master of Computer Applications, K.S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India.
Email : [1]sasicspsg@gmail.com, [2]aniraniraj@rediffmail.com

ABSTRACT

Wireless sensor network combine information sensing, wireless communication, information processing in current years. Two major constraints related to wireless sensor networks are the dynamic variance of the network caused by capacity constraint of sensor nodes and uncertainties related to wireless links. Moreover, the problem in wireless sensor networks is the active variance in topology and provisioning of secure routing. These problems are attributed to the strict constraint of sensor nodes' energy and the frequently variation of wireless channels qualities, which related with the nodes susceptible to energy failures and higher level of link prone from external interference. Certain works related to the hierarchical clustering did not address the problems related to the deployment model, efficiently on heterogeneous wireless sensor networks. Proposal of this work, introduces, Resourceful and Secure Routing Protocol (RSRP) for Wireless Sensor Networks based on Active Hierarchical Clustering mechanism (RSRP-AHC). Resource from the neighboring nodes serves as the dynamic information for the current network, with which sensor nodes make forwarding decisions based on energy aware and in a secure manner using RSRP. RSRP-AHC partition the nodes into clusters and select the Cluster Head (CH) based on the energy and Non Cluster Head (NCH) nodes join in the specific CH based on SNR values. Error removal during hierarchical cluster routing is achieved to avoid end to end error occurrence in network. Security is derived by isolating the malicious nodes using resourceful based secure routing pattern analysis. The experimental performance of RSRP-AHC mechanism is evaluated against Location-Based Pair wise Key Pre distribution model to attain packet delivery ratio, security level, and improved error recovery rate.

Keywords: *Hierarchical Clustering, Cluster Head, Sensor network, Resourceful and Secure Routing Protocol, Wireless Link*

1. INTRODUCTION

A typical wireless sensor network consists of densely positioned static sensor nodes with one static sink. The wireless sensed data are composed at the sink; sensors closer to the sink consume additional energy and have lesser lifetime. To overcome it the sensor nodes additionally positioned to replace failed sensors, or multiple mobile sinks are used. In a compound and huge building area, multiple heterogeneous sensor networks are positioned with a single point of sensed data collection named as gateway. In this case, sinks are sparsely positioned and located far from the gateway, so an energy efficient delivery mechanism from sinks to the gateway is required.

Homogeneous clustering protocols assume that all the sensor nodes are equipped with the same amount of energy and as a result, they cannot take the advantage of the presence of node heterogeneity [4]. Energy efficient heterogeneous clustered scheme for wireless sensor networks does not deal with clustered sensor networks with more than two levels of hierarchy and more than three types of nodes. Energy-aware clustering algorithm uses competing range to construct clusters of even sizes. At the same time, the routing algorithm increases forward tasks of the nodes in hardly covered areas by forcing cluster heads to choose nodes with advanced energy and fewer member nodes as their next hops [11].

Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks cannot perform more targeted attacks, and collide with other attackers to avoid intrusion detection [15]. An estimation scheme based on ambient noise floor and validate it further reduce estimation errors, identify an assessment feedback metric to enumerate the estimation errors and devise jammer localization as a non-linear optimization problem, whose global optimal solution is secure to jammers' true positions [16].

Homogeneous sensor network lifetime consists of like nodes and heterogeneous network lifetime consists of different type node points. In a heterogeneous lifetime model, it is composed of sensors without relaying functionality. Relay Nodes (RN) is used to obtain the information for the sensed data and for most favorable assignment. For this, RN between sinks and the gateway are used, but if static sinks are added vigorously the trajectory of mobile sinks cannot be identified. The most favorable placement of RN becomes a more complex problem than that for a single heterogeneous sensor lifetime. Two new random deployment policies, specifically the lifetime-oriented deployment and hybrid deployment exclusively aims at balancing the energy consumption rates of RN across the network, thus extending the system lifetime [20].

Energy efficient ant colony algorithms for data aggregation focus on balancing the energy cost of the entire network to extend the network lifetime whereas ACO does not obtain the lifetime into account [2]. Distributed Data Gathering Protocol (DDGP) was presented to address the problem of data gathering for a mobile sink. A k-hop relay mechanism was introduced to border the number of hops for routing data to a mobile sink. In order to increase the efficiency of the data gathering, a supportive environment between the sensor nodes and the mobile robot was presented to formulate the data gathering path. Cooperative environment failed to extend the algorithms for a mobile sink [3]. To diminish the communication energy consumption of the sensor node, the distance between the transmitter and the receiver was predicted in prior to obtain the transmission availability, and then, the lowest transmission power needed to broadcast the measurement information was determined [8].

Fault-tolerant relay node placement deploy a minimum number of relay nodes that establishes paths between every pair of sensor and relay nodes and partial fault-tolerant relay node placement, which aims to organize the smallest amount of relay nodes to achieve diverse levels of fault tolerance in the context of heterogeneous system [5]. In ongoing work pursue tighter performance ratios of the approximation algorithms, as well as enhanced heuristic implementations. Message in Message (MIM) allows a receiver to uncouple from a continuing reception, and connect onto a stronger incoming signal. Links that conflict with each other and it make concurrent nodes with MIM [10].

An active algorithm that opportunistically grabs packets from existing neighbors was developed. Under a simple model where each user desires a single file with infinite length, the algorithm was shown to optimize utility while incentivizing participation [17]. Combined and Differentiated Localization approach occur a tradeoff in the threshold settings [18].

Pocket Driven Trajectories (PDT) algorithm data collection technique allows information collection paths for monitoring query based on the spatial layout of selected nodes. First, the latency incurred by the PDT algorithm was studied by increasing the data collection path while decreasing the energy consumption [6]. The efficiency of data collection does not include spatio-temporal and model-based data suppression strategies. A Query-Centric Framework sensor network system does not support numerous users and applications. It was a motivating and important issue to tackle multiple pipelines for query processing in heterogeneous sensor networks. Moreover, as the data of a sensor network may be shared by multiple queries, the optimal schedule of a single pipeline does not match the optimal solution when it is scheduled together with other pipelines [12].

Queen-MAC independently and adaptively schedules nodes wake-up times, decreases idle listen and collisions, increases system throughput, and extends network lifetime. Queen-MAC was highly suitable for data collection applications and was not a flexible method for channel assignment that might have higher overhead, but it utilized additional channels [7]. In such channel assignment, nodes utilized the channel assignment method to allocate control channels. Then, nodes following on these channels decide the obtainable free channels for data communication. Internet Protocol (IP) version 6 over small power wireless personal area networks (6LoWPAN) was based on a cluster tree. In the cluster-tree repair algorithm, when a cluster head correlate node fails or moves, a new cluster head or cluster relate node was elected to maintain the cluster-tree topology.

Sensor wireless network is widely measured as one of the most significant expertise. The sensing electronics measure ambient conditions related to the environment surrounding the sensors and convert them in to an electrical indicator. In many WSN applications, the consumption of sensor nodes was performed in an ad-hoc fashion devoid of suspicious planning and engineering. The research addresses the prospective of association among sensors in data gathering and process the coordination of the sensing activities. However, sensor nodes were constrained in energy supply and bandwidth.

A mutual-information-based sensor selection (MISS) algorithm was adopted for participation in the synthesis process [13]. MISS allows the sensor nodes with the uppermost mutual information about the objective state to transmit data so that the energy consumption was reduced while the desired target position estimation accuracy was heavily met. The detection of faulty nodes was at the same time not an effectual range and possible precautions were taken against them. Fast Transmission to Remote Cooperative Groups cannot extract any useful information from the transmitted messages [19].

Energy conservation is critical in WSN replaces an option for sensors organized in aggressive environments. Generally, communication electronics in the sensor make use of most energy. A number of applications of WSN necessitate definite sensing, coverage and connectivity throughout its outfitted period. Death of the initial node might origin instability in the network [14]. Therefore, the entire sensor nodes in the network must be alive to attain the objective during that period. One of the major obstacles to make sure these phenomena is unbalanced energy consumption rate. Several models were proposed to recover energy utilization tempo such as clustering, secure routing, and information aggregation in sensor network but it fails in following the hierarchical form of clustering [1].

In proposed work, Resourceful and Secure Routing Protocol is developed in Wireless Sensor Networks and it is integrated with the SNR values. SNR value based Active Hierarchical Clustering mechanism (RSRP-AHC) partition the nodes into clusters and select the Cluster Head (CH) between the nodes based on the energy. Non Cluster Head (NCH) nodes join with a specific cluster head based on SNR values obtained during the hierarchical form of clustering. Error removing during hierarchical cluster routing itself keep away from end to end error occurrence (i.e.) malicious node. Security is achieved in RSRP-AHC by separating the malicious nodes using sink based routing pattern investigation.

Resourceful and Secure Routing protocol in wireless sensor networks utilizes resource information from all its neighboring nodes to obtain the present states of them. RSRP consists of local independent forwarding decisions based on current feedback information and prediction of future conditions. Hence in other words, highly dynamic changes of network topology will not apparently compromise RSRP performance as the resource information makes it more adaptable to the variance of network topology. To protect RSRP from routing attacks such as Sinkholes attacks, Keyed Individual Way Hash Sequence (Keyed-IWHS) identify malicious attacks and authenticate the resource from neighboring nodes. In addition, as it is frequent that base station owns dependable capacity because of the rechargeable energy offers its capacity is exploited to perform statistic computations and analysis in order to detect malicious nodes.

The contribution of Resourceful and Secure Routing Protocol based Active Hierarchical Clustering mechanism (RSRP-AHC) is as follows,

* Every sensor nodes with inadequate supply of energy senses the data and transfers the information to the CH.
* The base station in wireless network is positioned at a specific distance and each node has a predetermined number of broadcast power levels.
* Provide secure routing, where each packet transmission is based on the information provided by the neighbor.

Moreover, the sender selects the neighbors with an assessment function and places neighbor list in the packet header. In RSRP-AHC mechanism, neighbors on receiving the packet, include its resource in the ack frame and acknowledges the sender, and in the intervening time make independent decision of whether to forward the packets or not.

The rest of the paper is organized as follows. Section 1 describes about the diverse form of existing work with their limitations. Section 2 details the Resourceful and Secure Routing Protocol mechanism followed by the algorithm. Section 3 presents the effective results on the simulation parameter to attain security. Section 4 evaluated the performance with the table and graph values. The final section summarizes a beneficial solution with the malicious free nodes during hierarchical cluster routing in wireless sensor network.

2. DEVELOPMENT OF RESOURCEFUL AND SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

In this section, the development of resourceful and secure routing protocol for wireless sensor network is designed with the description about the phases involved in it is presented with the help of an architecture diagram. Followed by the five different phases involved in the development of resourceful and secure routing protocol for wireless sensor networks is presented.

The initial work related to the Resourceful and Secure Routing Protocol is to group the sensor nodes into clusters. Moreover, the clustering methods are categorized into static and active clustering. Our work concentrates on the active clustering that is aimed at minimizing the total energy spent during the arrangement of the clusters in a network.

The proposed system RSRP-AHC mechanism is integrated with the SNR values and its process is divided in to five different phases namely Initial Setup Phase, Energy based Cluster Head Selection Phase, Energy based Non Cluster Head nodes Phase, Data Forward Phase during hierarchical cluster routing, and Malicious Node Identification Phase. The flow diagram of RSRP-AHC mechanism is shown in Fig 2.1

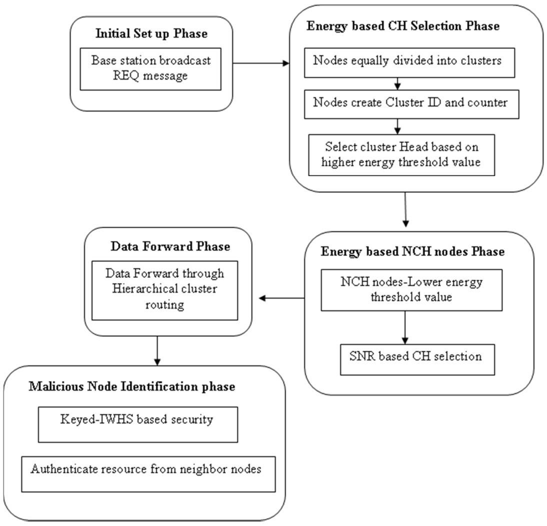

Initial Set up Phase
Base station broadcast REQ message
Energy based CH Selection Phase
Nodes equally divided into clusters
Nodes create Cluster ID and counter
Select cluster Head based on higher energy threshold value
Data Forward Phase
Data Forward through Hierarchical cluster routing
Energy based NCH nodes Phase
NCH nodes-Lower energy threshold value
SNR based CH selection
Malicious Node Identification phase
Keyed-IWHS based security
Authenticate resource from neighbor nodes

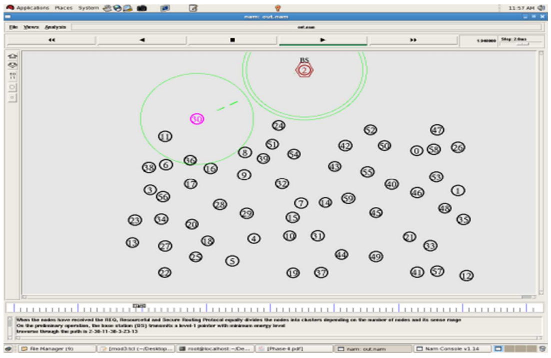
Fig 2.1 Flow diagram of RSRP-AHC Mechanism

Fig 2.1 performs the initial set up process, where the base station broadcast the messages to all the nodes present in the network with the help of REQ message. The next phase is the Cluster Head (CH) selection based on the energy threshold value. Initially, during the Energy based CH Selection Phase, the clusters are formed based on the nodes in the network and the CH is selected based on the higher energy threshold value. The nodes possessing lower energy value than the threshold value is the Non Cluster Head (NCH) nodes. The Data forward operation takes place using the hierarchical cluster routing that performs data aggregation function to compress the data into a particular pointer. The final phase identifies the malicious nodes to improve security level and authenticate resource from neighbor nodes.

2.1 Initial Set up Phase

The first phase involved in the development of RSRP-AHC mechanism is the initial set up phase. During the initial set up phase, deployment of the nodes, the base station broadcasts a request (REQ) message to every node. When the nodes have received the REQ, Resourceful and Secure Routing Protocol equally divides the nodes into clusters depending upon the number of nodes and its sense range. Each cluster frames its own Cluster Identity (CID) and the Cluster Counter (CC). The cluster counter maintains cluster head node number with its energy. In RSRP-AHC mechanisms, nodes which are alive, are considered as active nodes and which are turned off will be considered as sleep nodes. Primarily during the creation of cluster counter, the cluster head node number and its energy is set to zero value (i.e.,) null.

During the preliminary operation, the base station (BS) transmits a level-1 pointer with minimum energy level as illustrated in fig 2.2. All nodes which hear messages set their intensity value as 1.



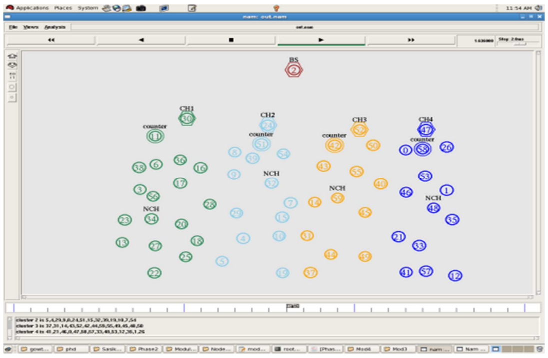
When the nodes have received the REQ, Resourceful and Secure Routing Protocol equally divides the nodes into clusters depending on the number of nodes and its sense range
On the preliminary operation, the base station (BS) transmits a level-1 pointer with minimum energy level
traverse through the path is 2-38-11-38-3-23-13

Fig 2.2 Base Station Transmitting Level-1 Pointer

During the next operation, the base station increases its pointer power to accomplish the next level and transmit a level-2 pointer. All the nodes that receive the message but do not set the preceding level set their level as 2. The process is repeated until the base station broadcast corresponding massages to all levels. The total number of messages of levels is equivalent to the number of distinct transmit pointer at which the BS sends. BS broadcast massage in Resourceful and Secure Routing Protocol, which contains the information of upper boundary and lower boundary of each level.

2.2 Energy based CH Selection Phase

The second phase involved in the development of RSRP-AHC mechanism is the Energy based CH Selection Phase. Every group in Resourceful and Secure Routing Protocol decide its cluster head based on its energy value. Among, all the nodes in the cluster, the node, which is having the utmost energy, is chosen as the CH as shown in fig 2.3 where three cluster head are selected namely, CH2, CH3 and CH4 respectively.



cluster 2 is 5,4,29,9,0,24,51,15,32,39,19,10,7,54
cluster 3 is 37,31,14,43,52,42,44,59,55,49,45,48,58
cluster 4 is 41,21,46,0,47,58,57,33,40,53,12,35,1,26

Fig 2.3 Three Cluster Head Selected

The subsequently highest energy node is selected as next CH, so that throughout the next iteration if the CH losses its energy the next CH becomes the current CH. The threshold form is defined in Eqn.1

$$S_i(m) =$$

$$\frac{(Q*P)(W_i - dis(m,BS))}{(1-Q)(t\ mod 1/Q)(w_i - K_i)} \left[\frac{F_{current}(m)}{F_{minimum}(m)}\right]^j$$

………….. Eqn (1)

Where, Q is the preferred percentage of the cluster heads with t denoting the present turns (i.e.,) overall round turns whereas t is the set of nodes, which have not been the CH in the last 1/Q turns. P is the constant factor between zero and one with W_i representing the upper limit of level-i and K_i being the lower limit of level-i and dis(m, BS) represents the position between node ‘m’ and the Base Station (BS).$F_{current}(m)$ denote the current energy of node ‘m’ with $F_{minimum}(m)$ as the initial energy of node ‘m’ and the power value of ‘j’ is between zero and three.

2.3 Energy based NCH Nodes Phase

The third phase involved in the development of RSRP-AHC mechanism is the Energy based NCH Nodes Phase. In the Resourceful and Secure Routing Protocol, communication between the cluster head and a node farther than the radio range of the cluster head is achieved through intermediate nodes (1-hop member nodes). The intermediate nodes which make available relay service is based on their signal to noise ratio value. If ordinary node receives a cluster head state message from the CH node and if does not belong to any other cluster, then it launches a confirm message to CH node. Now the Resourceful and Secure Routing Protocol standard node becomes a 1-hop node and generates its own ID and sends a situation message to its neighbors surrounded by their section.

If a NCH node receives a state message from a 1-hop member node, it will confirm itself as a 2- hop member node. The 2-hop member node also decide its own cluster identity ‘CID’, which is ‘m’ byte random integer added at the end of the selected 1-hop member node‘s ID. It infrequently happen that two sensor nodes within a same cluster choose the same random number. This type of divergence is solved by the cluster head by giving one of the nodes a different ID number. Upon completion of non cluster head phase, each node has unique ID number and is familiar with which cluster it fits into. The abdicate message is sent by each cluster head to notify its member nodes to serve as the cluster head in the next turn, because of their lower energy levels.

2.4 Data forwarding through Hierarchical Cluster Routing

Once the CH and NCH are formed, the fourth phase involved in the development of RSRP-AHC mechanism is data forwarding using hierarchical cluster routing, each cluster head creates a list of its cluster members. The information about the cluster members is broadcasted back to the nodes in the cluster. Once the clusters are created and list is fixed, the process of data forwarding is started. Each node sends data to its cluster heads with minimal transmission energy. The energy is estimated by received pointer strength of the advertisement message, so that data transmission uses a negligible amount of energy. Once the information has been received from the cluster members, then the cluster head node carry out data aggregation function to reduce the data into a single pointer. After a certain interval of time during the next turn, hierarchical cluster routing starts. After the cluster arrangement using cluster counter, the cluster heads broadcast the aggregate data to the subsequent level. At the subsequent level, the nodes aggregate their data and send to their cluster heads. In this manner, the cluster heads at the final stage broadcast the information to the BS with minimal energy consumption by removing the error nodes.

2.5 Malicious Node Identification phase

Finally, the malicious node identification is carried out. Generally, the attacked area contains many nodes and the intruder nodes are not necessarily located at the center of the area in a sensor network. Hence, it is necessary to position the exact intruders and isolate them from the network which is achieved by analyzing the routing pattern in the affected area. Based on the analysis RSRP mechanism protects from sinkhole attack, recognize the primitives to secure the resource information in wireless network. The most essential problem in securing the resource and making the insusceptible is how the sender makes sure that the resource is coming from justifiable neighboring nodes. RSRP-AHC adopts the Keyed Individual Way Hash Sequence (Keyed-IWHS) to address this problem.

Keyed-IWHS concept is of two levels sequence values$j_o, j_1, j_2, \ldots\ldots j_n$ and $j_0^{'}, j_1^{'}, j_2^{'} \ldots\ldots j_n^{'}$. For the first level, the root of the chain j_m is randomly chosen and kept as secret. Each value in the chain $j_i$is computed by applying n→i times of the individual way hash functionHF_1,

$$j_i = HF_1^{n-1}(j_n) \quad \ldots\ldots \text{Eqn (2)}$$

The one way hash functionHF_1, has the property that it is computationally infeasible to compute any j_i in a limited time. For the second level, each value $j_i^{'}$ is computed via

$$j_i^{'} = HF_2(G_{hj,}j_i) \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{Eqn (3)}$$

Where, function $HF_2$is a keyed individual way hash function and $G_{hj,}$is preconfigured global secret before network deployment known only to the legitimate nodes. Each sensor node ‘α’ holds the signature signed by the base station using the identity $ID_\alpha$and the Keyed-IWHS. The signature is used to authenticate the Key-OWHC, hence rejecting malicious nodes from creating their own unauthenticated individual way sequences.

2.6 Algorithm for Resourceful and Secure Routing Protocol based on Active Hierarchical Clustering mechanisms

The RSRP-AHC algorithm is described for collecting the network flow information.

```
Begin
Input: Base Station ‘BS’, Node ’m’, Cluster Head ‘CH’, Cluster Counter ‘CC’, Cluster identity ‘CID’, limit
Output: Secure network with authenticate resource from neighbor nodes
// Initialize set up phase
Step 1: BS broadcast REQ message
// Energy based CH selection Phase
```

```
Step 2: Node 'm' are divided into clusters
Step 3: Create CID and CC from cluster group
Step 4: Select Cluster Head based on energy threshold value
Step 6: If energy threshold value> limit
Step 7: Cluster Head Formed
Step 8: Else, all other nodes NCH nodes
// Energy based NCH nodes Phase
Step 9: Non cluster Head based on lower threshold value
Step 10: NCH node receives a state message from a 1-hop member
// Data forward Phase
Step 11: Establish Hierarchical cluster routing on active nodes
Step 12: Forward data packets from source node
// Malicious Node Identification phase
Step 13: Keyed-IWHS based security with two hash function 'HF1' and 'HF2'
Step 14: Authenticate resource from neighbor nodes
End
```

RSRP-AHC demonstrates a method for collecting the network flow information, which facilitates the routing pattern analysis. First, the Base Station (BS) sends a request message to the network. The message contains the ID of the nodes, and is flooded hop by hop. For each node receiving the demand, if its ID is present, then the node should react to the BS with a message, which includes its own cluster ID, the ID of the next-hop node, and the cost for routing, hop-count to the BS. Note that the next-hop and the cost could previously be affected by the attack; hence, the response message is transmitted along the turnaround path in the flooding, which corresponds to the original route with no attacks.

3. RESULTS ON USING RESOURCEFUL AND SECURE ROUTING PROTOCOL

Resourceful and Secure Routing Protocol for Wireless Sensor Networks using Signal to Noise Ratio (SNR) based on Active Hierarchical Clustering mechanism (RSRP-AHC) are evaluated using NS-2 to estimate the performance. For evaluation purpose, compared RSRP-AHC algorithm with the existing Location-Based Pair wise Key Pre distribution model [1].

The proposed RSRP-AHC mechanism is evaluated in an efficient manner using with 500 nodes in an area of 1000 * 1000 m. The security mechanism is evaluated efficiently in order to identify the malicious node while transferring from source to destination. The nodes' incoming time (sec) is noted as t1, t2….tn. The simulation results show that it takes 750 secs to transmit the packet securely from source to destination by choosing the path efficiently. The performance of the Resourceful and Secure Routing Protocol based Active Hierarchical Clustering mechanism is measured based on packet delivery ratio, security level, error recovery rate, in sensor network.

Packet delivery ratio in resourceful and secure routing protocol is defined as the amount of effective packet transfer from the source node to destination nodes. Data delivery ratio varies according to the size of the cluster, measured in terms of percentage.

$$Packet\ Delivery\ Ratio = \frac{No.of\ packets\ received}{No.of\ packets\ transmitted}$$

Security level is defined as the rate of malicious attacks such as sinkhole attacks that are removed from the wireless network. Malicious attack removed security level of RSRP-AHC and Location-Based Pair wise Key Pre distribution model is measured in terms of percentage (%). Error recovery is the rate at which the errors are recognized effectively while transferring the packets from source to destination while using the Resourceful and Secure Routing Protocol.

4. PERFORMANCE OF RSRP-AHC MECHANISM

Resourceful and Secure Routing Protocol for Wireless Sensor based on Active Hierarchical Clustering mechanism (RSRP-AHC) are compared with the Location-Based Pair wise Key Pre distribution [1] model. The table given below and the graph describe the performance of the RSRP-AHC mechanism against Location-Based Pair wise Key Pre distribution model.

Table 1 Tabulation Of Data Delivery Ratio

No.of Nodes		10	20	30	40	50	60
Data Delivery Ratio (%)	Existing Loacation – Based Pair wise Key Pre Distribution	76	79	79	80	82	83

	model						
	RSRP-AHC Mechanism	91	92	93	93	94	9

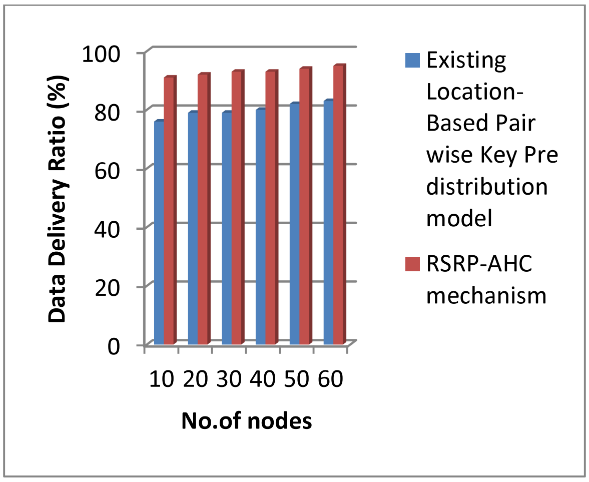


Fig 4.1 Measure Of Data Delivery Ratio

Fig 4.1 describes the measurement of data delivery ratio. Compared to the existing Location-Based Pair wise Key Pre distribution model [1], proposed data delivery ratio achieves 10 – 15 % better deliver rate. The data delivery ratio of Resourceful and Secure Routing Protocol for Wireless Sensor Networks is improved as all the information is received from the cluster members. Then the cluster head performs the data aggregation function to reduce the data time taken to deliver into a single pointer that improve the data delivery rate in RSRP-AHC mechanism when compared with the existing location based pair wise key pre distribution model. The variance achieved using RSRP-AHC is 10-15% higher than the existing Location-Based Pair wise Key Pre distribution model.

Table 4.2 Technique vs. Security

Technique	**Security (%)**
Existing Location-Based Pair wise Key Pre distribution model	85
RSRP-AHC mechanism	90

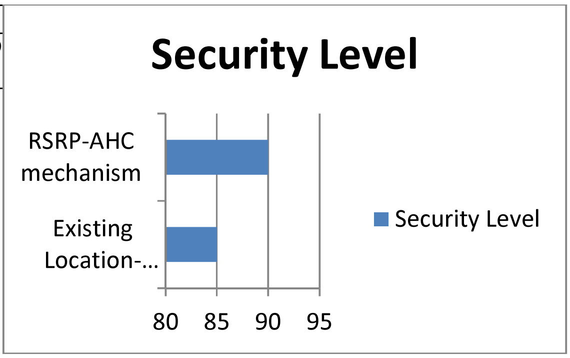


Fig 4.2 Measure Of Security Level

The security level of existing location based pair wise key pre distribution model and RSRP-AHC mechanism are examined and the output is measured in terms of percentage (%). Keyed Individual Way Hash Sequence (Keyed-IWHS) approach in RSRP-AHC mechanism improves the security level. The two way hash function HF_1 and HF_2 are preconfigured with global secret network deployment for security level. Consequently the security is approximately 5% improved in RSRP-AHC mechanism when compared with existing Location-based Pair wise Key Pre distribution model.

Table 4.3 Tabulation Of Error Recovery Rate

No.of Attack Nodes		3	6	9	12	15	16
Error Recovery Rate (%)	Existing Loacation – Based Pair wise Key Pre Distribution model	85	88	86	87	89	90
	RSRP-AHC Mechanism	90	91	89	91	92	94

Table 4.3 describes the error recovery rate based on the attack nodes. As the attack nodes increases, error recovery rate percentage of Resourceful and Secure Routing Protocol for Wireless Sensor Networks is also increased gradually from 89 to 95 % respectively. As the node attack increases, recovery rate of RSRP-AHC mechanism also gradually increases.

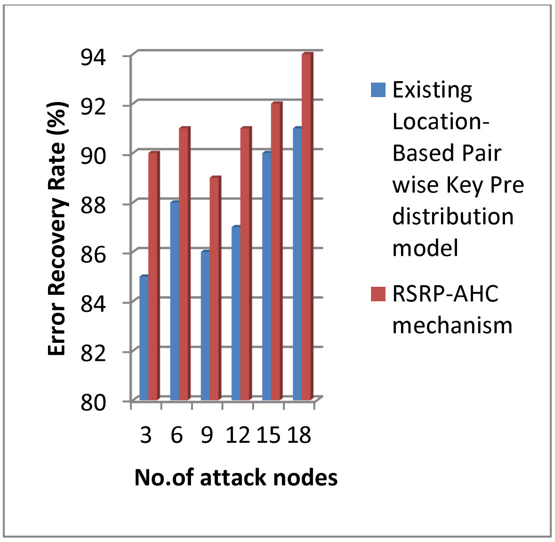


Fig 4.3 Measure Of Error Recovery Ratio

Fig 4.3 describes the error recovery ratio of the existing location based pair wise key pre distribution model [1] and RSRP-AHC mechanism. In RSRP-AHC mechanism, recovery rate is improved from 2 – 5 % when compared to the location based pair wise key pre distribution model because j_i and j_i' is computed by applying n→i times of the individual way hash function. j_i and j_i' computation easily identify the malicious attacks on the node, by accurately spotting the error in wireless network.

Finally, it is being observed that the RSRP-AHC mechanism in WSN, nodes is deployed uniformly at random position. All nodes have the same wireless communication variety in RSRP-AHC mechanism, follow the secure transmission. The proposed scheme leads to the efficient malicious node removal with prolonged lifetime when the network is congested.

5. CONCLUSION

Resourceful and Secure Routing Protocol serves as the dynamic information of the current network. SNR based Active Hierarchical Clustering mechanism (RSRP-AHC) performs the process with minimal energy consumption. RSRP-AHC partitions the nodes into clusters and selects the CH among the nodes based on the energy. Non Cluster Head (NCH) nodes join with a specific CH based on lesser energy threshold SNR values. Sensor nodes make forward decisions in a secure way using RSRP. Keyed Individual Way Hash Sequence (Keyed-IWHS) authenticate resource from neighbors, and use the statistic detection of base station to discover potentially compromised nodes, hence making RSRP resilient to existing routing attacks. The experimental result of RSRP-AHC mechanism attains the improved packet delivery ratio, security level and 3.285 % improved in error recovery rate. The process of separating the attack node further amplifies the number of hop count, which would further increase the delay in data delivery. Hence, node replacements strategies have to be examined carefully in future.

REFERENCES

[1] Taekyoung Kwon, JongHyup Lee and JooSeok Song, “Location-Based Pairwise Key Predistribution for Wireless Sensor Networks,” IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 11, NOVEMBER 2009, pp.5432-5442.

[2] Chi Lin, Guowei Wu., Feng Xia., Mingchu Li., Lin Yao., Zhongyi Pei., “Energy efficient ant colony algorithms for data aggregation in wireless sensor networks,” Journal of Computer and System Sciences., Elsevier journal., 2012, pp. 1686-1702.

[3] Kiran Mehta., Donggang Liu., and Matthew Wright., “Protecting Location Privacy in Sensor Networks against a Global Eavesdropper,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 2, FEBRUARY 2012, pp.320-336.

[4] Dilip Kumar., Trilok C. Aseri., R.B. Patel c., “EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks,” Computer Communications., VOL 32, No.4, MARCH 2009, pp.662-667.

[5] Xiaofeng Han., Xiang Cao., Errol L. Lloyd., and Chien-Chung Shen., “Fault-Tolerant Relay Node Placement in Heterogeneous Wireless Sensor Networks,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 5, MAY 2010, pp.643-656.

[6] Muhammad Umer., Lars Kulik, Egemen Tanin., “Optimizing query processing using selectivity-awareness in Wireless Sensor Networks,” Computers, Environment and Urban Systems., Elsevier journal.,VOL. 33, No.2 , MARCH 2009, pp.79-89.

[7] GholamHossein Ekbatanifard., Reza Monsefi., Mohammad H. Yaghmaee M., Seyed Amin Hosseini S., “Queen-MAC: A quorum-based energy-efficient medium access control

protocol for wireless sensor networks," Computer Networks., VOL.56, No. 8, Elsevier Journal., MAY2012, pp.2221-2236.

[8] Ruqiang Yan., Hanghang Sun., and Yuning Qian., "Energy-Aware Sensor Node Design with Its Application in Wireless Sensor Networks," IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 62, NO. 5, MAY 2013, pp. 1183-1191.

[9] Xiaonan Wang., and Huanyan Qian., "Constructing a 6LoWPAN Wireless Sensor Network Based on a Cluster Tree," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 3, MARCH 2012, pp.1398-1405.

[10] Justin Manweiler., Naveen Santhapuri., Souvik Sen., Romit Roy Choudhury., Srihari Nelakuditi., Kamesh Munagala., "Order Matters: Transmission Reordering in Wireless Networks," ACM journal., 2009, pp.

[11] Jiguo Yua., Yingying Qia., Guanghui Wangb., Xin Gua., "A cluster-based routing protocol for wireless sensor networks with non uniform node distribution," International Journal of Electronics and Communications (AEÜ)., VOL 66, No.1, Elsevier Journal., January 2012, pp.54-61.

[12] Yuan He., and Mo Li., "COSE: A Query-Centric Framework of Collaborative Heterogeneous Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 9, SEPTEMBER 2012, pp.1681-1693.

[13] Tolga Onel., Cem Ersoy., and Hakan Delic., "Information Content-Based Sensor Selection and Transmission Power Adjustment for Collaborative Target Tracking," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 8, AUGUST 2009, pp.1103-1116.

[14] Cunqing Hua., and Tak-Shing Peter Yum., "Optimal Routing and Data Aggregation for Maximizing Lifetime of Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 16, NO. 4, AUGUST 2008, pp.892-903.

[15] Hamid Al-Hamadi .,and Ing-Ray Chen., "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE transaction on Wireless network, VOL. 10 No. 2, JUNE 2013, pp.189-203.

[16] Zhenhua Liu., Hongbo Liu., Wenyuan Xu., and Yingying Chen., "An Error Minimizing Framework for Localizing Jammers in Wireless Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS SPECIAL ISSUE ON TRUST, SECURITY AND PRIVACY, VOL. X, NO. X, XXX 2013, pp.1-10.

[17] Michael J. Neely., "Optimal Peer-to-Peer Scheduling for Mobile Wireless Networks with Redundantly Distributed Data," IEEE TRANSACTIONS ON MOBILE COMPUTING, TO APPEAR., 2012, pp.1-13.

[18] Jizhong Zhao., WeiXi., Yuan He., Yunhao Liu., Xiang-Yang Li., Lufeng Mo, and Zheng Yang, "Localization of Wireless Sensor Networks in the Wild: Pursuit of Ranging Quality," IEEE/ACM TRANSACTIONS ON NETWORKING., VOL 21, No.1, 2013, pp. 311-323.

[19] Qianhong Wu., Bo Qin, Lei Zhang, Josep Domingo-Ferrer., and Jesús A. Manjón., "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 2, APRIL 2013, pp.621-633.

[20] Kenan Xu., Hossam Hassanein., Glen Takahara., and Quanhong Wang., "Relay Node Deployment Strategies in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 2, FEBRUARY 2010, pp.145-159.