Secure Data Accumulation among Reliable Hops with Rest/Alert Scheduling in Wireless Sensor Networks

Mohamed Mustaq AhmedA, Abdalla AlAmeen, Mohemmed Sha M, Mohamed Yacoab M.Y, Manesh.T
Computer Science Department,
Prince Sattam Bin Abdulaziz University,
Wadi Addawasir, Saudi Arabia

***Abstract*—Wireless Sensor Networks (WSNs) are more inclined to attackers by outer sources. The total information must be secured to guarantee the uprightness and privacy. In sensor networks, the data collection and data accumulation are mainly based on the energy levels of the sensor hops. Due to the drain of the energy, at one particular point of time the sensor hops become obsolete and the data transmission will not take place. This research proposes a reliable and secure strategy with dependable hops utilizing own-key logic test with convention for sensor organization. This research work proposes to practice a few hops as dependable hops (Reliable-hops) to understand the insight nature of the nodes. With every hop, a secret authorization is shared among the sink and its neighboring hops. At this point, a network is developed for sending information to the sink hops in a progressive design. The hops encode the information by utilizing the secrecy authorization and advances to the next level in network. By improving the transmission structure of reliable-hops, the accumulated value was confirmed towards guaranteeing trustworthiness. The proposed system is demonstrated with various examples and carried throughout the paper.**

Keywords—Sensor Networks; Data Collection; Data Accumulation; Reliability; Security Key; Rest/Alert hops

I. Introduction

A wireless operated dedicated sensor / actuator system is a future innovation, has sought out a wide significant thought by the research and expert group. A few little, minimal effort gadgets constitute the sensor arrangement, which is really a self-sorting framework. Its primary capacity to show the actual nature of data to at least one sink hops [1].

In remote sensor organization, the fundamental operations performed are identified with checking the physical environment, detected data handling transmission to the specific aggregator hops. Consequently, outlining a productive convention for expanding the system lifetime is the significance in this vitality obliged framework [2].

Due to the positive elements of Sensor Networks, this framework is generally used in variety of areas. For example, robotization, medicinal applications, ecological checking, fire control system and movement direction etc...

In WSN, to save the energy and the lifetime of hops there are multiple strategies are available. One most quality oriented service is implemented by sleep/awake scheduling in the sensor hops. In many different WSN real time applications, the sensor hops should be able to communicate at much faster speed to send the adequate and necessary data to the sink hops. In this context delaying the data transfer due to any means will not be tolerated at any case. This paper broadly discussed about how to minimize the delay in propagation of data from one hop to another hop. [19].

A. Methods in WSN

In sensor network there are two primary jobs one to just collect the data from the hops and the other the accumulating the data from the hops. The data collection just collects the information from the hops and transmits directly to the centrally located sink hops. While transferring, the data collection will also sends the duplicate data collected by temporal or spatial collection methods.

The data accumulation works is on two folds: data collection and data accumulation. While collecting all the data from the hops, it removes the duplicate data before sending the data to its sink hops. Hence the data focuses on distributed data processing and energy conventions on the sensor networks and reduces the conflict of medium access layer in networks significantly [3]. Ease of use, Privacy and Flexibility are the significant qualities presented by data accumulation.

At critical situation, the vital use of the data collected by the accumulation process may be adjusted due to lack of creation as well as preservation of well-defined network construction. Nevertheless, such tactics are irrelevant because of the unstructured activities such kind of organic hazard, chemical venture and smoke fire, are some evident factor over choicest data collected by accumulation.

B. Different kinds of Attacks in Sensor networks data accumulation

Service Rejection: It is popular attack in WSN; it obstructs the wireless frequencies that send the wireless flags in communicating system. From the setting of accumulation, denial of service can appear as aggregator that decays the total detected information. Because of this, the final goal is not reached by the hop.

Different style of occurrence attack: In this attack, the aggressor spreads numerous personalities of the traded off hop. By creating different personalities, the attacker makes an approach to give extra information in favor of malignant collector hops in accumulation choice procedure and chooses the malicious hop as a collector. The attack actuates the most noticeably bad state of system.

Progressive Attack: Here the assailant took the control over the messages sent and received in sensor network by compromising the hop.

Repeat Attack: An intruder monitors the entire network routing and its traffic and keeps an eye over it, and then the intruder uses the same in different parts of the network by varying time to time. This assault misguides the collector that leads to network conflict. [4]

C. Security Requirements in Sensor Networks

Information Veracity: Information veracity is the procedure of empowering the communicated message is unchanged, unmodified, cracked or hacked by the assailants.

Information Secrecy: Information Secrecy is termed as the ability of the system to shields up the communicating data from the opponent over the transmitting medium. This feature supports to send the message in secret.

Information Readiness: Checks the capability of hops to use different resources and it finds suitable way to send the data in the available sensor network. To preserve a sensor network the readiness of the network is the critical part.

Information Precision: This shows the precision of value collected in the aggregator hops. Information precision is a benchmark for collecting information in data accumulation system.

D. Problem Identification

Generally in WSNs the data collection using accumulation is more liable to security threats. Due to security threats, the intruder tries to steal, divert and misalign the data as well as disturbs the flow of the network traffic. To overcome this, a novel idea is implemented by sending the data in a secured manner across the wireless sensor network.

In this paper, the idea of rest/alert hops are dependable and the effective output will be utilized in the present directing multiple data convention for the similar cases of wireless sensor transmission, for example, State Election Protocol. This rest/alert procedure is joined with the secured accumulation and the paper emphasizes a few hops as dependable hops (Reliable nodes) to screen the procedure of data collection through accumulation. As an expansion effort, this result gives a solution to the previously mentioned issues, and recommend to utilizing a safe and solid information accumulation system that use dependable nodes with rest/alert nodes for Wireless Sensor Networks.

II. Related Works

Prakash G L et al. [5] have proposed a total plan protection for data collection through data accumulation functions. The Cluster-based Private Data Accumulation (CPDA) influences logarithmic properties of polynomials and grouping convention. The aim is to overcome any issues among the data gathering by WSN and information protection. Furthermore, this method has crucially proved that they use minimum amount of transmission work.

M. Bahi et al. [6] have developed a protected information system works with a minimum vital key using elliptical cryptography on an end-to-end basis. Also, the plan permits the usage of maximum number of different tasks on encoded messages. It keeps the exact refinement among indistinguishable data within encoded messages. In addition, this method allows to use the minimum encoded keys, the key is so vital in the WSN.

Inria et al. [7] presented an encryption system that permits an effective data collection of encoded information. The security of their plan depends mostly on the attribute of a pseudo random function (PRF), a customary cryptographic method. On the way to ensure the uprightness of the collected information, the authors have developed a conclusion for total verification that is safe in contradiction of attackers. The projected method is reasonable for processing measurable qualities, for example, mean, difference, and standard deviation of detected information, while accomplishing huge data transfer capacity is achieved.

Huang [8] had projected a protected encoded data collection for remote sensor systems. Their proposed approach for data collection removes the duplicate sensor readings without utilizing encryption and keeps up information with high level of secret and privacy.

Ozdemir et al. [9] designed Data Accumulation and Confirmation convention, called DAC. The DAC is planned to incorporate wrong data location with data collection and classification. In order to cope the data collection with erroneous data identification, while observing hops of each information aggregator conducts data collection also generates tiny message authentic codes for data validation and verification. It also enables the high level confidential data transfer between two data collection hops on an encoded fashion rather than normal plain text.

Lin [10] proposes an n-dimensional strategy for protecting data privacy accumulation scheme in WSNs. The sensor has the capability of storing multiple values in the hops. By doing so, the energy used by the sensor hops will be retained for longer periods.

Zhijun Li et al. [11] put forth a method using the cryptic hash function to concise reasonable protected method of data collection by joining the with Bloom channel. This method is a powerful data collection method that is reasonable for a particular yet famous class in remote sensor systems. The preferred usage from secure Bloom channel, with no improbable presumptions, it satisfies the crucial security target of avoiding outside intruders internal hops from hurting the general system output.

Di Pietro et al [12] illustrated a method based on the idea of delayed data collection with peer checking of local hops. This method highlights the confidentiality and integrity of data collected through different data collection sensor networks. If the hops are under attack, then the hops will provide only the minimal numerical data, after detecting that the hops are under attack this provides a high security to adjacent sensor hop to protect the data loss from the attacked hops.

Haifeng Yu [13] has proposed a tree-testing method of calculation that specifically utilizes to answer the data collection inquiries and gives subjectively enhanced usefulness in connection to the existing secure data collection techniques. The primary favorable position fathoms an important key test examining by reducing the direct problems into mathematical based problems that uses logarithms as the process models. This method influences with certain properties of sampling viz., (such as nice and clean security techniques) to achieve the final stages of the goal proposed. By using a guaranteed sampling technique which eliminates the problems associated with sampling and thus making this approach an effective one when the number of inputs to the predicate functions is more.

Kavita Sharma et al [16] propose a method that will take into account, the energy levels of the hops prior creating the group hops. In this paper, concept of rest/alert method which uses the rest hops of high energy efficient and also high reliable source hops in the wireless sensor network transmission.

III. Suggested Solution

A. The Insight Details of the suggested system

Illustrated in a greater vision, this paper proposes to execute a safe data system with dependable hops utilizing key predicate test technique with rest/alert method for sensor systems. Consider all the sensor hops are static. A static sink is situated amidst the system hops. The hops equipped with full charge, hold the abilities to shift their charged levels to the adjacent hops. Every node detects the residual energy that it holds has the information to send to the sink station. The strategy practices a few hops as dependable hops which confirm the procedure of data accumulation. At first, by using stream cipher techniques, every hops produces a couple of keys, which is shared among sink station and adjacent hops. The data collector network is developed to send information to the sink in a multilevel structure. Accumulated data is encoded by utilizing secret code and advances to the next level. Prior sending data to the next data collector hop, the accumulated data value is checked with the data collected by reliable hops. If both data are equal, then the node is not under attack. If both data are not equal then the data by default becomes illegitimate, shows that the hops are under attack. The secrecy key is made available among neighboring hops, the possibility of hops to be traded off by intruder. Subsequently, hops with vital information key are kept at high vigil utilizing own-key predicate test. Hops that fulfills logic key test are set to red color and other different hops as yellow color. The hops which are marked by yellow color will not be considered for data collection and transmission of the sensor network.

B. System Design of the Network (FRAMEWORK)

Let us have the sensor network with n-number of sensing hops distributed in WSN sensing area. Every hop captures distinctive events. The captured data by the sensor hops by means of data accumulation are sent to the sink hop (Base Station) progressively. This method is utilized for the data collection and a network structure is built according to the sensor network. The network design is appeared in figure-1. All the hops are assumed to send the data to the sink hop within a random time period; subsequently, all the sensor hops are inherently works with synchronized clocks.

Data transfer Technique in WSN

The data transfer technique in WSN is majorly classified into three types, a Simple transmission design, Mmultilevel routing technique, Position based Routing techniques.

Simple transmission design

The basic class of routing protocol is the mutihop single transmission protocol. In single transmission protocol, every sensor hops coordinate to perform the sensing task in the sensor network. Due to multiple number of sensor hops, it is not possible to assign a common unique identifier to every hop. Due to the above problem which leads to a data centric routing in which the sink hops transmit signal to various areas and as well as in this particular areas, the sink hop anticipates for the data from the hops[17].

Multilevel Routing technique

The multilevel routing technique works with the concept of clusters in which every hop lies within WSN area are gathered together along with its adjacent hops creating a group called cluster. The data gathered by the sensor hops which originally belongs to the cluster are not sent to sink hops directly instead the data collected within that group creates a cluster head. The data collected are finally assigned to a group head that will send the data to sink hop. By doing so, the energy levels can be saved significantly. The multilevel routing techniques are divided into two major categories such as centralized and non-centralized routing techniques [20].

Position based Routing techniques

Sensor hops are location specific. Based on the signal strength, the adjacent hops distances are calculated. By reading the data of the adjacent hops, the data can be exchanged among adjacent hops either spatial or temporal [18].

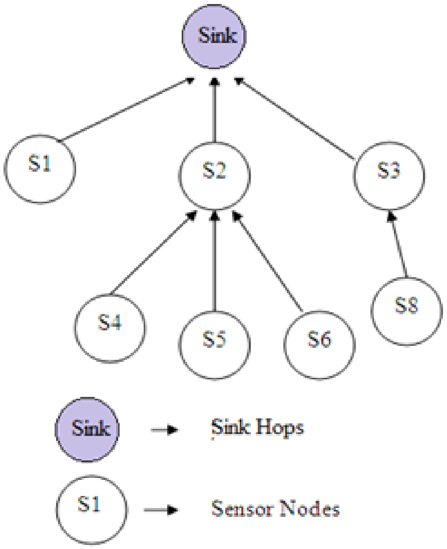

Fig. 1. Aggregation Tree Structure

C. Protected Key generation and sharing

At this point, it is expected that every hop creates a key stream utilizing SNOW [14] termed as stream cipher system. The secrecy key SKi is processed and imparted to sink hops and furthermore with adjacent hops. The pairwise key sharing technique is used to share Ski to its adjacent hops [15].

The network hops are helpless against security as information sent across the span of sensor network. The data collected from hops are sent over the sensor network are secured using probabilistic encryption function. Let's take KW () as probabilistic encryption function. Assume ZKi be the protected key and F be the data to be transmitted. At that point, KW () with m can be derived as,

$$\text{KW}\ (F1, ZK1, m) = F1 + ZK1(mod\ m) \qquad (1)$$

Where m = modulo function

This additive homomorphic encryption scheme, used with probabilistic encryption function KW () is given as

$$KW\,(F1, ZK1, m) + KW\,(F2, ZK2, m) = (F1 + ZK1\ (mod\ m)) + (F2 + ZK2\,(mod\ m)) = F1 + F2 + ZK1 + ZK2\ (mod\ m) = KW\ (F1 + F2,\ ZK1 + ZK2,\ m)$$
(2)

D. Data Collection with Reliable-hops

In these multilevel routing techniques, every hop can be either a data collector (Ai) or a Reliable hop. The hop Ai gathers information from numerous sensor hops (Si) in one level (a) of total network and advances to next higher level (a + 1). The detected information is sent from low level hop to the sink hop. The sink hop is the root.

After defining an aggregator (Ai) and Reliable node(R-node), an additional hop called as supplier hops (Pi) also defined, the Pi is used to collect data from the sensor hops and encrypts using the secret key ZKi and sends the data to the data collector (Ai).

With regular interval t, the supplier hops Pi (i=1, 2 ...n) is sending the data to the data collector node (Ai) in the specific three fold formats (PE_{Pi}, $PR_{Pi,}$ PN_{Pi}).

Where,

PE_{Pi} ⟶ Encrypted value of supplier hops P_i
PR_{Pi} ⟶ received data collection value of P_i
PN_{Pi} ⟶ Number of supplier hops

Taking the data from each supplier hop, the new accumulated value PNAi is generated. The PNAi is created will be defined as follows,

$$\text{PNA}_i = \frac{\sum_{p=1}^{n}(\text{PR}_{\text{pi}} * PN_{pi}^{-1}) + \sum_{p=1}^{n} PE_{Pi}}{n} \qquad (3)$$

Where n represent as $n = n_{p1} + n_{p2} + \ldots + n_{pn}$

During the calculation of PNAi at regular interval t, the any one of following two conditions can occur,

a) All supplier hops (Pi) at stage a will send data to collector hop Ai

b) A few supplier hops at stage a will not send its data to collector hop Ai

The data transfer from the supplier hops to collector hops will not take place when there might be no data transmission during that specific time interval. In that condition, the collector hop (Ai) includes secrecy keys (ZKi) of those sensor hops with new data accumulation function. At that point, KNAi is encoded by applying nonce value (N) and number of supplier hops (n).

Designing of Reliable-hop Set

The procedure of Reliable-hops helps to authenticate the exactness of accumulation function carried out by the data collectors. The Reliable-hops diagram is depicted below in Figure-2.

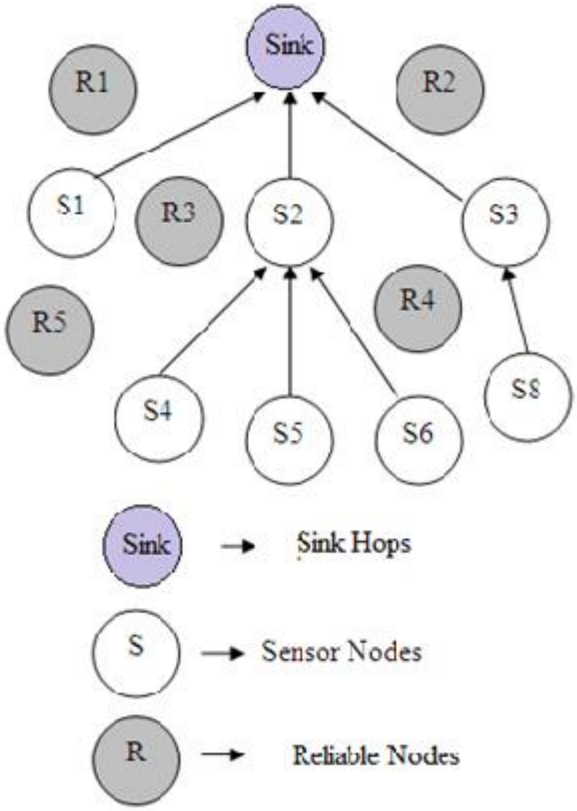

Fig. 2. Network with R-hops

The Reliable-hop set of data collector is indicated by Я (Ai). It incorporates the adjacent hops of Ai, which are not belongs to collection tree. The set (Ai) is made known to collector hops (Ai) and all Reliable-hops. This method ensures that all the supplier hops of (Ai) are equally known to all Reliable-hops.

Each elements of network hop is working under radio broadcast communication environment, every Reliable-node could catch the action of its adjacent hop. Similar technique is also used in data collector hops, every Reliable-hop can gather similar information collected by its adjacent data collectors.

Hence, this data collecting hop can assist Reliable-hops with verifying the collection procedure.

At the point when Ai is aggregating the data, the related R-node also collection the data, after time interval t, the gathered data of Ai and Ri are checked for equality. On the checking the data of Ai and Ri, the output of the hops are genuine only if both Ai and Ri are equal. If they are not equal, then the output of the hops are not genuine and the hops are under attack.

Design of working model -1

Let PNAi be the accumulated value of Ai

And Ri be the dependable node of Ai and PNRi be the data collected of Ri

In the event (PNAi = PNRi)

Here verification is true, Hops are authentic

Otherwise

Authentication is false, Hops are not authentic

In the situation when supplier hops of Ai are inside the scope of Ri, then the data collection verification process will take place by the approach given above. At this point, within the scope of transmission, when Reliable hops does not have straight communication with supplier hops of Ai, and then Ri plays out the data collection within maximum two hops.

E. Own-Key Logic Test

Illustrated in section 3.3, every hop has a secrecy key and that is shared between the sink hops and the adjacent hops. There are chances that hops can compromised by the intruders by false key, making the entire network under attack. Meanwhile a time interval t, the sink hops cross examine the secrecy key of the sensor hops for the exactness. In order to achieve this process, the sink hops uses a test called own-key logic test.

An own-key logic is defined as, $KP(S_p) = KP(S_q)$ (4)

p and q are data inputs and S is the number of device-sensors. The design makes use of two colour to explain (red and yellow) as two input data. By the outcome of own-key logic test, hops are set apart with different color. Hops that fulfill the own-key logic test are colored with red and hops which do not fulfill the own-key logic test are colored in the yellow.

At first, all hops remain uncolored. Hops having the key ZKi need to fulfill the test called own-key logic test. Consider every hop has different name as per their key value. Rather than utilizing the key deliberately, the sink uses distinct key parameter name given to sensor hops. As the initial stage of own-key logic test process, the sink communicates own-key logic communication to all hops in the system. The communication message incorporates the hops key name ZKi, the nonce value (N), the own-key logic and Message Confirmation Code (MCC) of N

$$\text{Sink hops} \xrightarrow{message} \text{All hops}$$

The sensor hops containing the secrecy key satisfies own-key logic test, sense the data back to the sink hop as a mark of reply. It is already discussed that hops are marked with red and yellow color to define the authentic and non-authentic hops respectively. After transmitting a message from own-key logic test the sink hop waits for a period of time, t, comes to the conclusion, whether the data sent by the hops are authentic or not, by differentiating the input color of the hops. The following is presented well in figure 3.

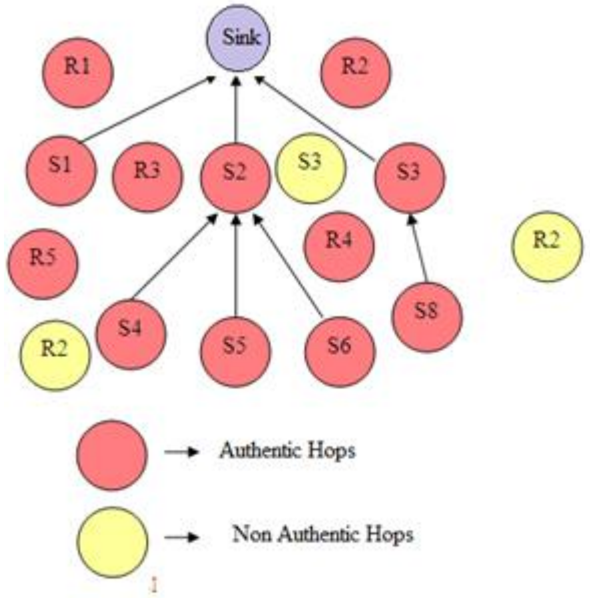

Fig. 3. Own-Key Logic Test

In the above figure 3, clearly illustrates the own-key logic test procedures. Hops with red shades are accumulated into the data collection system and hops with yellow shade will be discarded.

Design of working model -2

The proposed work plan to be incorporated (ALGORITHM -2)

A static sink is situated at the network's center

Hops were enriched by suitable electrical abilities can differ with the broadcast energy.

Each node detects network by the speed and dependable information send to the sink.

1) The data broadcast channel should be balanced. Hence, the power needed to send a data from input to a goal hop is the same as the power needed to send a similar data starting from the goal hop to input hop for a given Signal to Noise Ratio (SNR). The data transmit by the hop does not need retransmission because the broadcast environment is high contention and error free.

2) Let assume the sensor hops are scattered over the network in a random manner. Let u hops are in the network, out of that a small number of hops, termed as t hops are set with more energy in the multiples of α than the rest of the hops. The high energy hops termed as hi-energy hops and the rest hops are called as normal-hops, given by the formula (1-t) x u.

3) To begin with, the initial energy of the normal-hops is set to Ko. The energy for hi-energy hops can be calculated by using the term Ko x (1 + α). The entire aggregate strength of the new varied setting is equivalent to: u * ko * (1 + α * t)

So by using the term (1+ α * t), the overall energy of the system is increased so that there will be a high reliability of data transfers within hops.

a) Every hop which termed as normal hops will be converted into a group head hop after each pt * (1+ α * t) times; here pt means prob. to the group head hops.

b) Every high-energy hops will be converted into a group head precisely (1 + α) times at each one pt· (1+ α * t) iterations

c) The average number of group top hops / cycle / time period = u × pt

4) The selection of group head for the normal-hops is based on the following formula

$$T1\left(S_{nrm}\right)=\frac{P_{nrm}}{1-P_{nrm}.\left(\mathrm{r}\ .\mathrm{mod}\frac{1}{\mathrm{Pnrm}}\right)}$$

$if\,snrm\in \mathrm{H}G'$; normal – set of normal hops

0 $otherwise$ eqn (1)

Where r is the present cycle,

HG' - set of normal hops that are not able to be the group heads till the last **1**/**P**$_{\mathrm{normal}}$rounds,

T1 (S$_{\mathbf{n}\mathrm{ormal}}$) is the value of threshold applied to the accumulated population by the factor u x (1 − t) (normal) hops.

This above formula ensures that every normal-node will turn into a group head precisely under every (1.0/ pt) x (1+ α * t) iterations/cycle, and the average number of group head hops which are normal-hops per round is equivalent to n x (1.0 − t) × pnormal.

5) The Selection of Group head hops for high-energy are calculated by the formula cited below:

$$GT2\left(GS_{progressivenode}\right)=\frac{GP_{progressivenode}}{1-GP_{progressivenode}.\left(\mathrm{r}\ .\mathrm{moduulus}\frac{1}{\mathrm{GPprogressivenode}}\right)}$$

Sprogressive nodes ∈ HG'' ;

GSprogressive node – set of advance or next hops in the network

0 $otherwise$ eqn (2)

Where HG" is the set of hi-energy hops that are not able to be the group heads within the last GPprogressive node iteration

GT2 (GSprogressive node) is the value of the threshold applied to the populace of u x t (high-energy) hops.

This above formula ensures that each high-energy hop will turn into a group head precisely at every (1/pt) x (1+α * t) / (1+α) iterations.

6) In the view of conditions cited above, hops transmit the data value /information to their group heads and the energy utilized by the hops are ascertained as

J**node** = **k**. (J**Tx**. (**l**, **d**) + J**amp**) eqn (3)

7) The accumulated data will be collected and transmits to the sink hop by the group heads and energy utilization by the hop shall be figured out for every hop and every group head.

J**cluster** = **k**. (J**Tx**.(**l**, **d**) + J**Rx**.(**l**) + J**DA** + J**amp** eqn (4)

8) By utilizing the probability conditions, in next cycle, the normal-hops will be converted to be group head hops.

9) By determining of the group head hops, Hops transmit the information to their group head hops, chosen by the criteria of having the relatively smaller distance of a specific hop of the group head and the energy utilization can be computed.

*10)*Group head hops shall sum up the aggregated information and transmits it to the sink hop and the required amount of energy can be calculated.

*11)*Certain numbers of the hops say "q hops" will put under the rest mode to improve the sensor network's life span and also to preserve their energy levels which are less than 1 Joule. In event that the more numbers hops are required for data transmission , then the nodes are brought in to dynamic action from the rests state to dynamic active state that directs the information to adjacent group head hops.

*12)*This procedure will go through the entire system until the said performances are reached in the data transmission.

IV. Advantages of the Projected Structure

With the implementation of reliable node, it can able to track the intruder and locate the attacked hops.

By comparing the data values of both accumulated data and the data in the reliable hop with the key values, it could reach the maximum accuracy of the data being transmitted, makes the data under secured transmission,

By implementing the own-key logic test, the keys are accurately validated leaving no room for nodes comprising under keys.

Using rest/ awake strategy in secured data transfer in the Wireless Sensor Networks, hops lifetime, the residual energy will be maximum and the lifetime Performance will be more for the information to be transmitted.

A. Setup required for model design

Description	Values
Total No. of Hops	50
Size of the area	700 X 700
MAC address	802.11
Imitation Time	30 sec
Transportation Source type	CBR
Capacity of Each Packet	512
Transmit Power in watts	0.661 w
battery Power received in watts	0.396 w
battery Power in idle state in watts	0.036 w
Energy at initial stage measured in joules	10.1 J
Range of Transmission	75m
Total base stations	2
Total number of sources	4
Total number of data collector hops	6
Node values	Multiples of 2 and more..

B. Measuring the Quality Factors

Normal data Distribution Ratio: Proportion to the incoming data packets over the aggregate amount of data packets sent.

Power Consumption: It is the normal setup, that every hop will consume battery power for transfer of data to its neighboring hops, receiving data from other hops or any kind of service that took place in the network.

Data Loss/Failure: It's clear, that the normal amount of data packets / parcels failed to reach data collector hops because of attacks carried out by assailants.

C. Outcomes and Outputs

A detailed comparison is made through a graph for the different levels of attackers with various operational overheads such as assailant with packet drop and delivery, amount of power and energy used etc. The assailants are taken in multiples of 2… and so on.

The performance, quality factors are compared with the existing algorithm which works secured data transfer with reliable hops are compared with secured data transfer with sleep/ awake hops methods are illustrated as follows.

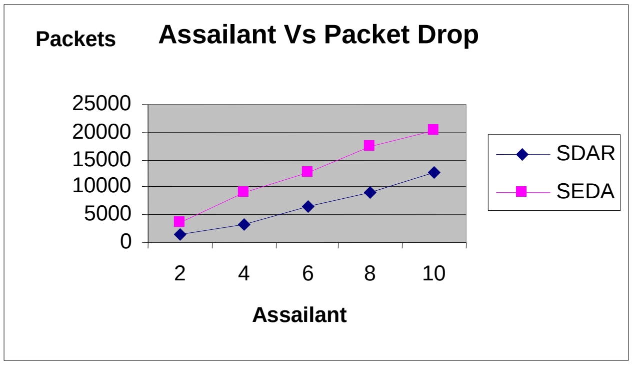

Fig. 4. Assailant Vs Drop

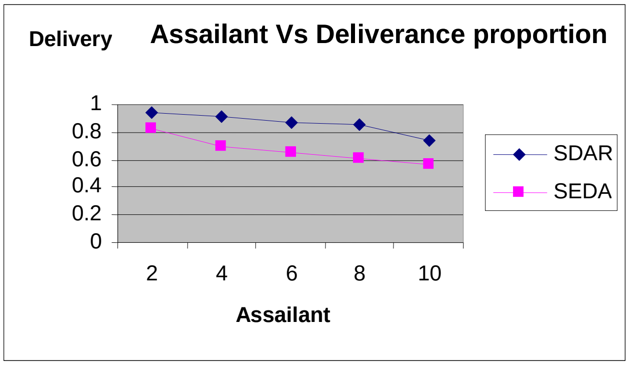

Fig. 5. Assailant Vs Deliverance proportion

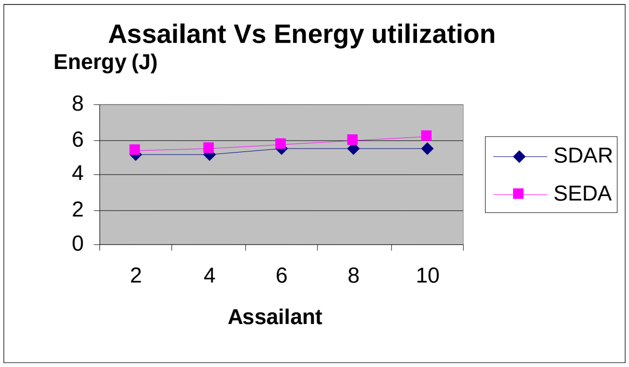

Fig. 6. Assailant Vs Energy

V. Conclusion

This research framework proposes the concept of rest/alert methodology to secure the data accumulation using own-key logic test with reliable hops. Here the hops are put to sleep and whenever it is needed they are dynamically activated, thereby save the energy of the hop tremendously. Using the above said framework, it is possible to compare the reliability and saving the energy on hops with some of the existing routing protocols. In this proposed work, certain hops as reliable hops that look after the job of the data aggregator. Between the hops and the sink hop, a secret key to be shared and all the hops know the value of the keys. After sharing, a tree is generated to transmit the data in a multileveled manner to the sink hop. The data collector hops encodes information utilizing secrecy vital key and advances to a next stage in collection network. The data collected by the reliable hops are checked for consistency and integrity by increasing the transmission attribute of reliable hops. The validity of the key is checked using the own-key logic test. By simulation, this strategy is finally demonstrated. The result proves there is a subtle increase in the data delivery ratio, thereby minimizing the data packet loss considerably. As a future work, this research can be extended with the implementation of dynamic robust key management system for securing sensor hops which have a greater impact in saving the hops from the intruder attacks.

References

[1] Dorottya Vass and Attila Vidacs, “Distributed Data Accumulation with Geographical Routing in WSN”, Pervasive Services, IEEE Intl Conf., 08 Augt 07.

[2] Cunqing Hua and Tak-Shing Peter Yum, “Optimal Routing and Data Accumulation for Maximizing Lifetime of WSN”, IEEE/ACM TRANS. ON NETWORKING, VOL. 16, NO 4 AUG 08.

[3] Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, “Optimal Policies for Dis. Data Aggr. in WSN”, Draft Infocom2007 Paper.

[4] Dr. G. Padmavathi and Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in WSN”, (IJCSIS) Intl Jour of Comp Sci and Infn Security, Vol. 4, No. 1 & 2, 2009.

[5] Prakash G L, Thejaswini M, S H Manjula, K R Venugopal and L M Patnaik, “Secure Data Accumulation Using Clusters in Sensor Networks”, World Academy of Science, Engg and Tech, 51, 2009.

[6] Jacques M. Bahi, Christophe Guyeux and Abdallah Makhoul, “Efficient and Robust Secure Accumulation of Encrypted Data in Sensor Networks”, SENSORCOMM, 4-th Int. Conf. on Sensor Tech and Appl, Italy, 2010.

[7] Claude Castelluccia, Inria, Aldar C-F.Chan and Einar Mykletun, “Efficient and Provably Secure Accumulation of Encrypted Data in WSN”, ACM TRANS. on Sensor Networks, Vol. 5, No. 3, Article 20, May 2009.

[8] Shih-I Huang, Shiuhpyng Shieh and J. D. Tygar, “Secure encrypted-data accumulation for WSN”, Science+Business Media, LLC, Springer, 2009.

[9] Suat Ozdemir and Hasan Çam, “Integration of False Data Detection with Data Accumulation and Confidential Trans in WSN”, IEEE/ACM TRANS. on networking, Vol-18, No- 3, JUNE 2010.

[10] Xiaodong Lin, Rongxing Lu and Xuemin (Sherman) Shen, “MDPA: multidimensional privacy-preserving accumulation scheme for WSN”, Wireless Comm Mobile Comp,843–856, 2010.

[11] Zhijun Li and Guang Gong, “On Data Accumulation with Secure Bloom Filter in WSN”, 2010.

[12] Roberto Di Pietro1, Pietro Michiardi and Refik Molva, “Confidentiality and integrity for data accumulation in using peer monitoring”, Security and Comm Networks, 2:181–194, 2009.

[13] Haifeng Yu, “Secure and Highly-Available Accumulation Queries in Large-Scale Sensor Networks via Set Sampling”, IPSN '09 Proceedings of the 2009 Intl Conf. on Infn Processing in Sensor Networks, San Francisco, California, USA, Pages 1-12, 2009.

[14] Patrik Ekdahl and Thomas Johansson, “A new version of the stream cipher”, Proceeding of the 9th Annual Intl Workshop on Selected Areas in Cryptography, pp- 47-61, (SAC '02), 2002.

[15] Dijiang Huang and Deep Medhi, “Secure Pairwise Key Establishment in Large-scaleSensor Networks: An Area Partitioning and Multi-group Key Predistribution Approach”, Jour. of ACM TRANS. on Sensor Networks (TOSN), Vol 3 Issue 3, Aug 2007.

[16] Threshold based Routing Protocol for with Sleep/Awake Scheduling , Kavita Sharma Research Scholar, Department of Elec & Comm Engg. Panipat Inst of Engg & Tech Samalkha, Panipat, India IntlJournal of Comp Appls (0975 – 8887)Vol 133 – No.1, Jan 16.

[17] R. Yadav, S. Varma, N. Malaviya, “A Survey of MAC Protocols for WSN,” UbiCC Joul, 2009, Vol. 4, Issue 3, pp. 827-833.

[18] Rashmi Ranjan Sahoo, Moutushi Singh, Biswa Mohan Sahoo, “A Light Weight Trust Based Secure and Energy Efficient Clustering in Wireless Sensor Network: Honey Bee Mating Intelligence Approach”, Intl Conf. on Comp. Intelligence: Modeling Tech. and Appl. (CIMTA), 2013.

[19] Babar Nazir,Halabi Hasbullah1 and Sajjad A Madani , Sleep/wake scheduling scheme for minimizing end-to-end delay in multi-hop WSN EURASIP Jour. on Wireless Comm. and Network. 2011.

[20] S. Ehsan, B. Hamdaoui, “A Survey on Energy-Efficient Routing Tech. with QoS Assurances for WMSN,” IEEE Comm. Surveys Tuts., 2011, Vol. 14, Issue 2, pp.265-278

[21] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, “Energy-Efficient Routing Protocols in WSN: A Survey” IEEE COMM. SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[22] Brahim Elbhiri et. Al. “Developed Distributed Energy-Efficient Clustering (DDEEC) for heterogeneous WSN”, IEEE 2010.