A Novel Method formulated on Secure Clustering and Secure Routing(SCSR) to bring forth advanced security for Hierarchical WSN's

Mr. Irshad
Research Scholar
Department of ComputerApplication, Silver Oak University, Gujarat.

Dr. Premal Patel Associate Professor, Department of ComputerApplication, Silver Oak University, Gujarat.

Dr. Kinjal AdhvaryuProfessor,
Department of Computer Engineering, Shankersinh Vaghela Bapu Institute of Technology, Gandhinagar,Gujarat.

ABSRACT:

A Sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc. The output of the sensor is generally an electrical signal that is transmitted to a controller for further processing. In this research paper we have proposed a method using SCSR technique for providing high security to Hierarchical WSN's. In this proposed method, the dynamic key administration technique SCSR for heterogeneous mobile wireless sensor networks provides security framework which can be applied for medium and large scale applications that require security in all aspects. Includes the heterogeneous BNs used by the PSO technique in the network. BN nodes use EBS to perform stable clustering. The experiment is carried on simulator NS2 which shows the conceptual results that in compared with existing technologies, SCSR consumes lower processing and requires minimal communication costs for sensor nodes. When comparison to the cost of the backbone nodes, the connectivity cost for the cluster heads is also smaller. The findings of the simulation show that the software introduced issafer and the overhead is minimized. SCSR provides a good packet distribution ratio because of the multi-dispersal routing technology.

Keywords: Wireless Sensor Network, SCSR, Packet Delivery Ratio, EDDK

1. Introduction

Sensors are small strategies that are used to sense the real world attributes such as temperature, humidity, flow of air andwater, vibration, etc. In recent years, many applications use these sensors to predict the real world happenings and necessary actions are taken by the applications accordingly. Instead of using the sensors directly in the field, they are fabricated in the electronic devices called sensor nodes. The sensor nodes are the devices that consist of processing unit, memory, one or more types of sensors, battery and transceiver. An example node is shown in Figure-I.

Figure I: Sensor Node

The design of a sensor node is given in Figure-II. Many such sensor nodes spatially dispersed in the environment which working together are called as Wireless Sensor Network (WSN). The sensors in the WSN track interest phenomena and transfer information collecting data from sensor nodes to a single or more sinks or bases (BSs).

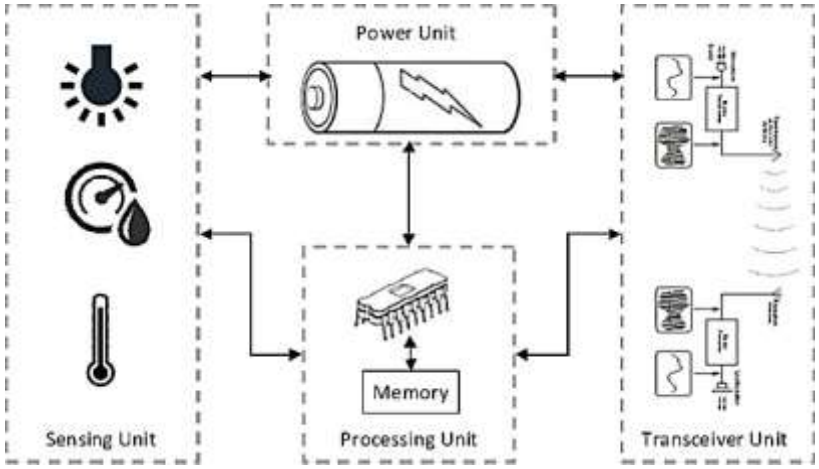

Figure II: Design of sensor node

Challenges in WSN

There are many challenges in WSN which are the conversion of raw data to digital form, robust operation, openness and heterogeneity, security, real-time and control, harsh environmental situations, reliability and latency supplies and packet mistakes. As the sensor nodes are smaller in extent, they are highly constrained in its resources such as energy, memory, transmission& reception range and computation capability. Among all these resources, energy is considered as a major factor to spread the lifetime of the system. The sensor nodes are organized in the arena of an unattended area for many requests such as animal habitat checking, forest fire finding, military surveillance, under water checking, etc. There is no energy source available other than the battery influence. So the energy should be efficiently used. A sensor node contains of both volatile Random Access Memory (RAM) and non-volatile memory (Flash Memory) with minimum capacity. In the non volatile memory the evidence such as program, node-ID, routing counter, and security connected data can be deposited. Other than this information, the sensor node has to maintain the application specific information such as keying information for providing security in its non-volatile memory. Since the capacity of the memory is very less, the program and the application specific information should not be overloaded.

There are various parts in a sensor node that consume power. Among them, only the transceiver consumes more power. While designing protocols for WSN, the number of message transmissions should be minimized to attain the task without compromising the objectives of the system. Subsequently the sensor nodes are untethered and unattended; they are susceptible to node capturing attack. From the captured node, the private data can be easily retrieved by the intruders and used to disrupt the service of the network.

Applications of WSN

WSN is one of the important technologies that is used in wide variety of applications. Presently there are different areas where WSN can be applied are given below:

A. Military Applications

WSNs are first introduced for military applications. The different types of military operations which use WSNs are battlefield, urban, OTW and force protection. Further the applications in military can be categorized based on the kind of sensors used to find the presence of intruders, CBRNE detectors, ranging, imaging and noise detection.

B. Health Care Applications

As a result of recent microelectronics development, medical sensing is becoming increasingly popular and highly used by people in hospitals, homes, workplaces and elsewhere. The technology enables the individuals to continuously measure physiological parameters such as heart rate, physical activity monitors and Holter monitors by wearing the sensors externally. These wearable sensors are also used to monitor the soldiers in the battlefield; computer-assisted rehabilitation and therapy; chronically the ill patients and to track the movements of sports players.

C. Environmental Applications

The applications of WSN in environmental checking can be generally considered as indoor and outdoor applications. Among these, the indoor applications include SMART home, SMART office, fire detection and civil arrangements deformations detections. The outdoor applications comprise Chemical dangerous detection, weather forecasting, detection of natural disasters and habitat monitoring.

D. Industrial Applications

WSNs are used in industrial applications based on the requirements of the industrial production. The three different classifications of IWSN are environmental sensing, condition sensing and process automation.

Network Architecture WSN

In general, a WSN collects information from sensor nodes, executes simple processing and refers it to the BS or Sink. The sensor nodes use either single or multiple hops to access the BS or Sink through intermediate nodes. And for very small applications can the single-hop systems be used. Each node should use long-range transmission to access the BS directly in this single-hop architecture. The diagram shows the layout of the single-hop long-haul network.

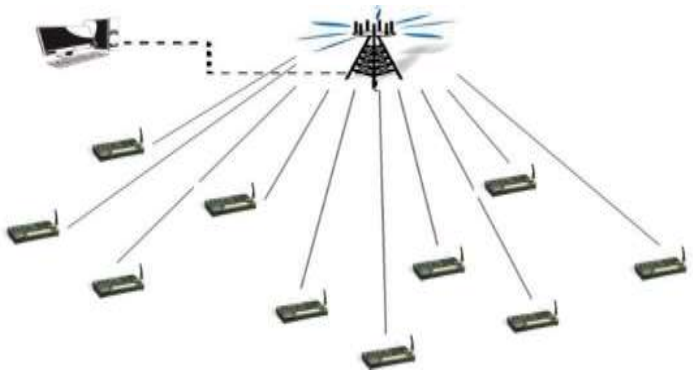

Figure-III. Layout of single-hop long-haul network

This long-distance transmission consumes additional energy and so the period of the network will be less. To solve this issue, the network uses multi hop short-distance transmission to send data to BS via one or more intermediate nodes. This type of transmission spends less amount of energy to transfer the data using short-distance communication. This multi-hop design is classified into two types: flat and hierarchical designs.

Flat Architecture: All nodes in the network play a similar role in this form of architecture, and nodes are also identical. The figure demonstrates the classic WSN flat architecture.

Hierarchical Architecture: The nodes in this structure are clustered into clusters in which the members ' nodes collect information and forward this information to the CH leading node which is in the same cluster. The CH receives the information from its representatives and, if necessary, processes it and sends the information to the BS or Sink. Usually lower-energy nodes are cluster members while larger-energy nodes serve as CH. This figure shows the typical structure of a single hop clustered WSN.

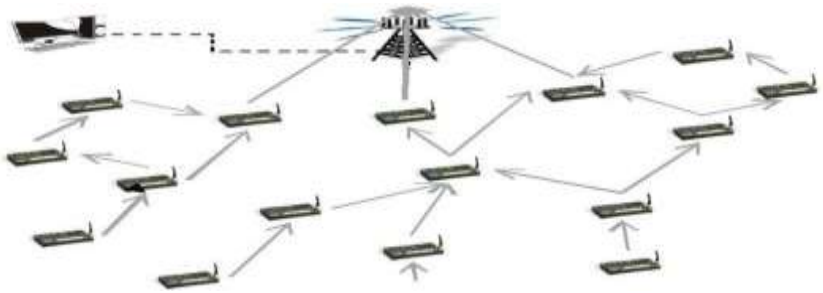

Figure-IV: typical structure of a single hop clustered WSN

The main benefit of the clustered design is its scalability. At the same time, the major issue of this type of architecture is that a few nodes have to act as CH also. As only a few number of nodes always act as CH, the energy in these nodes deplete quickly. To overcome this issue either the role of the CH should be rotated frequently or the nodes that are actingas CHs should be highly configured with long life battery storage in order to extend the life time of the network. The earlier case network is called as homogeneous system whereas the latter is called as heterogeneous network. The heterogeneity can be either link heterogeneity or energy heterogeneity or processing heterogeneity or memory heterogeneity.

Security in WSNs

WSNs are mostly operated in hostile environments. As the sensor nodes use wireless radio for communication, they can be simply

attacked by the adversaries. To fulfill the objectives of the WSNs, the security must be incorporated in the network. Safety is a problem in WSN's because of the limitations such as network size and density. As sensor nodes are installed in an unattended zone, it is also impossible to provide physical security. Given the nature of wireless communication, topology can not be expected before deployment.

Security Requirements in WSNs

The primary goal of the WSN security services is to defend against opponents ' information and property.

- ***Network and data availability***: The network should ensure the availability of services and data to the application in the presence of adversaries.
- ***Authorization*****:** The network should ensure that only the approved nodes should involve in providing data to the application.
- ***Authentication*****:** The network should ensure that only the legitimate nodes should participate in providing network service.
- ***Confidentiality***: The network should ensure that the transmitted data would be known only to the authorized nodes.
- ***Integrity***: The network should confirm that the transferred data should not be modified by the adversaries.
- ***Non-repudiation***: The network should guarantee that any authorized node should not deny the transfer of data that theycreated.
- ***Data freshness***: The network should ensure the freshness of the data.
- ***Robustness***: The network should ensure that the service of the network should be provided even a few nodes in the network were cooperated.
- ***Self organization***: The nodes in the network should be flexible by self-organizing themselves to provide service to the application.
- ***Time synchronization***: The network should ensure the synchronization of time among all the nodes in the network to produce correct data.

Attacks in WSNs

WSNs are susceptible to numerous types of attacks. Based on the safety requirements, the attacks are categorized into the following groups.

- ***Outside Attacks****:* The attacker nodes do not belong to a WSN.
- ***Inside Attacks***: The legitimate nodes belongs to a WSN perform illegitimately.
- ***Passive Attacks***: The attacker nodes simply watch the message transactions inside the WSN. They do not modify thedata.
- ***Active Attacks***: The attacker nodes modify the data and some times generate false data inside the WSN.

Hierarchical key management

In hierarchical key management systems, the keys are distributed centered on the hop counts by the clustered architecture. The network that provides in-network processing considers this key administration scheme. The nodes in this key management arrangement are arranged in various levels hierarchically where it consists of different types of nodes based on their capability. Mostly the nodes in the higher levels are highly configured and the lower levels are low configured.

Advantages**:** The storage in the network is carried out efficiently. There are localized keys necessary for the lower sensor nodes, prohibiting compromised nodes from affecting legal nodes.

Disadvantages**:** The nodes have to maintain different keys to join with diverse sorts of nodes at different levels. The nodes at the middle level should be secure more and highly configured in order to preserve the availability of the services at the leaf nodes.

2. Security Framework for Hierarchical WSNs

Introduction

Mobile sensor nodes require separate services from one location to the further, wherever they are, in a mobile wireless sensor network (MWSNs). Thanks to the movement of network nodes, fire reply, target tracking, detection of dairy cattle health and healthcare surveillance can be used in structuring emergency response. Other large scale applications like military surveillance, high level security for health care monitoring, SMART city etc. require huge number of nodes with different configurations need

to be deployed in the field along with mobility support. Every wireless sensor node could be mobile in the future omnipresent environments. When nodes pass from place to place the security of nodes must be guaranteed, confidentiality of communication and information integrity. The authenticity and privacy of all communications exchanged during the cross-cluster routing should also be maintained. Due to their complex topology, secure HWSN routing protocols have other challenges. In its proposal for an asymmetric key system and a symmetric key for the information security sector, Ozgur et al. suggested a multi-level hierarchical key management scheme. The UAV is used as an asymmetric key transmission and co-ordination center that reduces total processing, communication and sensor node computation. A flexible key management system in WSN that is polynomial and cluster-specific is primarily focused on energy efficiency but lacks security, as the current CH will not authenticate the key update. For WSNs for deterministic purposes, EDDK is a divided key management framework. This focuses both on the key development and on preserving the keys which also include local clusters.

For secure communication in WSNs, a symmetric key-based security architecture was introduced. This mechanism uses three keys which are the password, the lock key and the lock key. The key is exchanged with the BS, the cluster key is used in a cluster, and the cluster key is used in certain clusters between all the nodes. This framework, however, does not attain the least overhead storage. Jiun et al.' proposed to combine the nodes centered on average energies that are the same, an energy-efficient protocol for multi leive HWSNs. This work uses WSNs on two, three and multi-level scales to prove that their approach is time-consuming. The nodes closest to the BS are easily exhausted in most wireless sensory networks. A topology training scheme has been proposed to overcome this problem. The backbone tree is designed using strong nodes. This solves the problem of the hot spot.

Secure Clustering and Secure Routing

Under the proposed SCSR, the BNs conduct a stable clustering method with the Exclusion Basis system. The CHs are designated based on the value Wi weight, determined with ND, BN (DBN) Length, Sav and VBP parameters. Then the members of the cluster measure the CCV by NL, ND and VBP. The CCV is also used for dynamic keys generation. The secure management of the cluster is carried out if the node is transferred from one cluster to another. If information is to be moved from source to sink, safe route discovery within the clusters is carried out.

Network Architecture

To meet the necessities of the large scale HWSN, the network architecture should be designed hierarchically. Also different types of key management should be provided at various levels to meet the safety of the whole network. The architecture proposed is composed of BS and sink, BN, CH and n number of nodes (Nj), where j= 1 to n. These include BS and BNs, which are known to be healthier than CHs and member nodes. The capabilities of the CHs are very high in energy and computing power compared to the member nodes. The BNs are constant, the CHs often instead of sometimes. It is impossible to predict topology in advance. BNs are deployed on the network using PSO technology. The architecture suggested is outlined below.

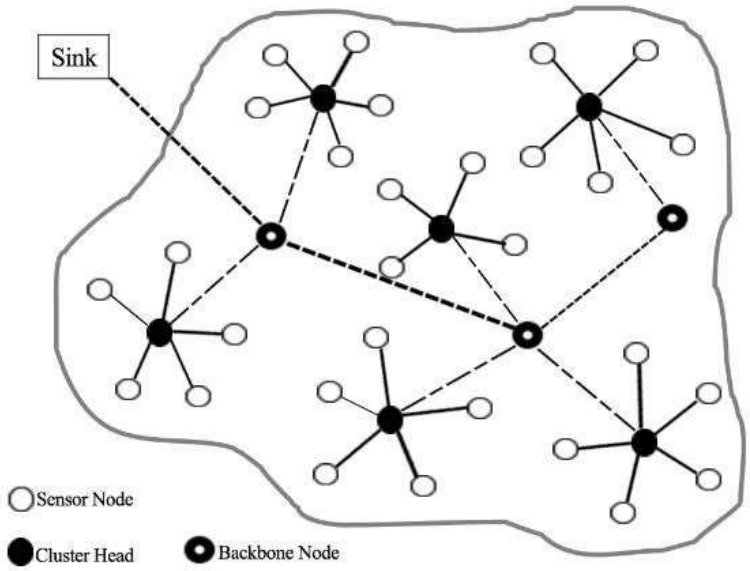

Figure V.: Deployment of BNs on PSO Technology

Exclusion Basis System

Each node requires administrative keys to be assigned to the methodology of the Exclusion Basis System (EBS). EBS is well-defined as the EBS (T, A, B) wherever T is the number of users allowed, A is the numbers of key for each subparagraph and B, but not within the subparagraph, is the numbers of key in an overall key set. The key advantage of the method is its reduction in key numbers and message recovery. Thus= A+ B is the global admin key array. The following example illustrates the EBS process. Research that in the array there are ten nodes with the following keys.

Node N1, N2, N3, N4, N5, N6, N7, N8, N9, N10

Key

K1 1 1 1 1 0 0 0 0 0

K2 1 1 1 0 0 1 1 1 1 0

K3 1 0 0 1 0 1 1 1 0 1

K4 0 1 0 1 10 1 0 1 1

K5 0 0 1 0 1 0 1 1 1 1

Note that N1 is affected. The same K1 and K2 keys are used by N1, N2 and N3. It includes a redistribution of thesebuttons.

The K4 U K5 set is the known key set for all associates other than N1. Therefore, during the re-keying of the corresponding M1 and M2 messages, these keys were used.

M1 = E (K4 (Kses, E(K3 (K3')), E (K2 (K2')),E (K1(K1'))

M2 = E (K5 (Kses, E(K3 (K3')), E (K2 (K2')), E (K1(K1'))

In K1, Kses = Session Key = where E (K1 (K1 ')) is K1 ' encryption.

These messages ensure that new keys are deciphered only by confident nodes. Therefore N1 is excluded and the K1, K2and K3 ' new keys are made existing in the K1, K2 and K3 keys.

Dynamic Key Management

We use the dynamic button, which changes for each session, in the projected design for intra-cluster message. The remainder of the battery power is increasing after each operation is carried out in the node. The current battery power cannot be correctly measured with the source and the endpoint nodes. Thus, the source and destination nodes could not use this value for dynamic key generation. Therefore, VBP is considered a commodity used instead of actual battery power. It is presumed that when it is initially deployed, every sensor node will have a digital battery power cost. The switch in VBP is used to dynamically measure the keys for communications within the cluster.

The location is focused on the DRL scheme in this architecture. For use in the DRL system, BN is called a seed node. Each NL node's location is determined by its codes (x, y). The ND is calculated founded on the information from the neighboring nodes. As a static network is constant in its location and node degree, both NL and ND values remain static. VBP varies according to node status, it is dynamic in nature. The value feature is changed whenever the VBP is decreased and values for î±, β, μ, a, and b are 0.3, 0.3, 0.4, 0.5 and 0.5.

Forward secrecy: The member node that leaves from a group should not be able to entree the credentials once it leaves from the group. It is called as forward secrecy.

Backward secrecy: When the new person enters a party, the previous qualifications should not be seen. It is called the secrecy behind it. The dynamic keys are generated from VBP costs automatically. There are no existing or new keys as the VBP shifts by transaction. Consequently, the technology preserves privacy.

Secure Clustering

BNs deployed in the HWSN were part of the proposed architecture. BN has high capacity for transmission. The number of BNs to implement is rational straight to the number of network nodes. We also conclude that the BN nodes information has been disappearing.

BN Deployment using PSO

The evolutionary computing method, known as PSO, is used to determine the best locations of BNs in the network, based on the bird flocking theory. Random startup of a number of nodes is originally handled. For each node, the fitness value for each generation is determined by the fitness function. It lets us know the best position that is called pbest and the natural position among the whole team is called gbest.

Notation Description

pbest define Local best

gbest define Global best

C1, *C2 is* Acceleration coefficients

W is Inertia weight

Vid is Velocity of element id

Xid is a Position of element id.

Sdis Short distance initial sensor node to BNLd is a Distance starting *BN* to *BS*

Which Electronics EnergyAnd Amplifier constant

F shows Fitness function

The node flight is guided by the node speeds. In each generation, the speed and location of the nodes are changed. In the equations,however, the velocity and location calculations are determined.

$$V_{id}^{(k+1)} = w \cdot V_{id}^{(k)} + C_1 \cdot rand_1(pbest_{id} - X_{id}) + C_2 \cdot rand_2(gbest_{id} - X_{id})$$

$$X_{id}^{(k+1)} = X_{id}^{(k)} + V_{id}^{(k=1)}$$

Increasing node is identified by us in the trouble spot, and the solution to the location is feasible. All components of the sensor are the same and the BN components are better than others. The best positions of the BNs can be established in a sensor network to reduce energy use.

Assume that within the zone, the sensor nodes will be short Sd-to-BN while every BN will have long Ld-to-base station. To send a b-bit message, the radio will expend on each Sd-to-BN sensor node:

$$\eta_s^{(b,Sd)} = b\,\eta_{elec} + b\,\rho_{fs}Sd^2$$

For BN, though, to communicate a b-bit communication with a distance Ld to base station, the radio spends:

$$\eta_L^{(b,Ld)} = b\eta_{elec} + b\rho_{mp}Ld^4$$

In both gears, to obtain the message, the radio spends:

$$\eta_R^{(b)} = b\eta_{elec}$$

Under take p clusters through h cluster members. Then the fitness function is consequent as:

$$F = \sum_{j=1}^{p}\sum_{i=1}^{h}(0.01Sd_{ij}^2 + \frac{1.3\times10^{-6}Ld^4}{h_j})$$

The fitness feature is described so that the normal nodes can be smaller distance away from the BN while the base station remains extensive than the BN. Therefore the nodes can be associated with the BN, which delivers an effective sensor network coverage.

Secure Clustering Phase

The Secure Clustering phase begins after the deployment of the nodes in the network after a certain period of time (our estimation is 120 seconds). This method is carried out to form network clusters.

Notation Description

Nj jth Node

KN is a Network Key

*BNi ith is a*Backbone Node

PKBiMj is a Pairwise key among*ith* Backbone Node and *jth* Member Node

PKBij is Pairwise key among Backbone Nodes

HPtx is a High transmission power*R_Mes is a* Reply Communication*A_Mes, Alive*

NDj is a Node Degree of *jth* Node

E{x} K Encrypted message *x* using the key *K*

Initialization

[Pre-conditions: the BS key pool is KN, PKBij and PKBiMj,] [Post-conditions: the BS key pool has consistentlybeen dispersed to all BNs and nodes of membership: KN, PKBij and PKBiMj]

1. Start
2. Load into every nodes the *KN,* assigned by *BS,*
3. Based on *BS,EBS,* or BNi*: E {*Set of *PKBij} ;{*Set of *PKBiMj } KN*
4. End

Cluster Formation

[Post-conditions: (1) Clusters were safely formed [Pre-conditions: Initialization has been done and trustingis given to all nodes]. (2) All nodes of members are aware of their CH]

1. Start
2. *BNi* broadcasts *{A_Mes}:* inside *BNi's HPtx* range,
3. *Nj, BNi : R_Mes|| BNi ||Nj||E{ BNi||Nj||x||y}KN*
4. Each *BNi* calculates *ND, BNi Nj : E{ID* of *BNi} ||ND|| {PKBiMj} KN*
5. Each *Nj* computes *Wi* as

$$W_j = \frac{(c_1 \times D_{BN}) \times (c_2 \times S_{av})}{(c_3 \times ND) \times (c_4 \times V_{BP})} \begin{cases} if\ S_{av}\ is\ 0, & set\ S_{av} = 0.1 \\ else\ S_{av} = current\ value \end{cases}$$

The c1, c2, c3 and c4 values shall be considered respectivly 0.20, 0.45, 0.25 and 0.45. Preferably the Sav,advanced VBP and fewer DBN node with lower mobility should be selected as CH.

6. *Nj BNi : E{ID of Nj || Wi } PKBiMj*
7. *BNi* selects *CH* consuming the function *Min (Wj),* some where *i=1..n*in its transmission area.
8. *BNi* transmission *CH* information Ni Nj
9. End

When node systems are ready to deploy in the network, a number of pairs of keys between BNs and sensor nodes just between BNs using the KN are securely loaded by the BS. The secure clustering process was initiated after the network was deployed. Each BNi transmissions A Mes to all nodes inside the broadcast range of HPtx during the Secure Clustering phase. The nodes will send R Mes to KN encrypted BNi after receiving A Mes, containing the node ID and

location of that node. BNi calculates the Member nodes and communicates it together with the pair key encrypted byKN after getting R Mes from every of its neighbors. Each NJ then calculates weight according to parameters including node rate, BN length, average battery speed and digital power. Each Nj detects its value to BNi, coded between itselfand the BN by a parallel key. BNi selects the CH node with the smallest weight value when gathering the encrypted weight values from the entire NJ and transmits them to its members.

3. Theoretical Analysis

In this section, we theoretically examine the suggested SCSR framework and the existing key management system EDDK based on the metrics such as storage above and communication costs.

Existing work used for Comparison

For comparative study, the existing key management scheme EDDK has been considered because it supports node mobility and provides secure key management. EDDK also does not depend only on the BS and mobile robots for secure key management and data transaction.

Storage Overhead

Store Overhead is known as the store space in the memory of the nodes engaged by various kinds of keys. The rankingof the overhead storage estimation and evaluation is as follows.

Notation DescriptionSCSR

n, k are the No of *SNs, and* No of *BNs* in the network

*m is*No of *SNs* in every cluster, *m=n/kNBK is a* Number of *BNs*

OvNj is Storage Overhead at *jth SN OvN is a* Total Storage Above at all *SNs*

Dij is a Dynamic Key between node *i* and *jOvBNi is a* Storage above at *ith BN*

OvBN is a Total Storage Above at all *BNs*

EDDK

Kab is a Pairwise Key

Ka is a Individual Key *KBa is a* Local Cluster Key*PT is a* Public Key

Storage OverheadSCSR

Key size of *EB 32* bits and *Dij 64*bits

OvNi = Scope*(KN)* + Scope*(PKBiMj)* + Scope*(Dij)OvN = n* × *OvNj*

OvBNi = m × Scope*(PKBiMj) + k* ×Scope*(PKBij)OvBN = k* × *OvBNi*

EDDK

Key scope 160 bits

OvNj = Scope*(Ka)* + Scope*(Kab)* + *Scope (KBa)OvN = n * OvNj*

Communication Cost

The over-head for communication between Sink, BN, CHs and Sensor Nodes is defined as the messaging cost. Theratings used to calculate and analyze the cost of communication are as follows.

Notation Description

CC1, CC2,CC3 and CC4 Communication Cost at Sink, *CH* at BN and SN respectively

q is No. of *CHs*

TxP is a Transmission Power for *1* bit of data is *0.074Wï is* Distance among *SN and BN*

ö is Distance among *SN and CHó is* Distance among *BN* and *CH*

nb No. of BNs among source *CH* and *SinkRtx Transmission variety in meters* ***Communication Cost***

SCSR

Network Key Distribution *CC1 = n* × Scope*(KN)* × *TxP****CC2 Calculation***

Pairwise Key Distribution

CC2 (4) = m × *(ï* × *Scope (PKBiMj))* × *TxP*

Cluster Maintenance

CC2 (3) = (ö × Scope (*Enc (Move_Req))) × TxP*

Secure Inter-Cluster Routing

CC2 (2) = 2 × (nb× Extent*(Enc (RREQ)) × TxPCC2 (1) = 2 × (nb* × Extent*(Enc (RREP)) × TxPCC2 = CC2 (4) + CC2 (3) + CC2 (2) + CC2 (1)*

CC3 Calculation

Cluster Maintenance

CC3 (4) = (ó × Scope*(Move_Req)) × TxP*

Secure Inter-Cluster Routing

CC3 (3) = (nb × Scope*(Enc (RREQ))) × TxPCC3 (2) = (nb* × Scope*(Enc (RREP()) × TxP*

Secure Data Forwarding

CC3 (1) = (nb × Scope*(Enc (Data))) × TxP*

Total CC3

CC3 = CC3 (4) + CC3 (3) + CC3 (2) + CC3 (1)

CC4 Calculation

Sending Encrypted Weight Values to BN

CC4 (1) = (ï × Size *(Enc (Wi))) × TxP*

Sending Encrypted Data to CH *CC4 (2) = (ö× Enc (data)) × TxP*Total CC4

CC4 = CC4 (1) + CC4 (2)

EDDK

Pairwise Key Updating

CC1 (1) = (ï × Size *(Kab)) × TxP*

Cluster Key Updating

CC1 (2) = q × (ö × Size *(KBa)) × TxP*

Join Request Transmission

CC1 (3) = (Rtx × Size*);(JREQ) × TxP*

Join Request Answer

CC1 (4) = (Rtx × Size*); (JREP) × TxP*

Total CC1

C1 = CC1 (1) + CC1 (2) + CC1 (3) + CC1 (4)

4. Simulation Study

The implementation of the proposed framework SCSR is done in C++ and verified in NS2 with 2.32 TCL simulation scripts. The performance of SCSR and EDDK are tested in a number of simulated scenarios. The simulation scenarios have been created by changing the number of nodes and the topology of the network.

Network Threat Model

Our objective is to ensure clustering and routing safety. The size of the network comprises 100, 200, 300, 400 and 500 clusters and BN nodes. Because the nodes in BN use the PSO system, only 2% of the overall network size is needed for the required BNs. Use of the safe clustering process to form clusters after deployment of BNs. If the cluster Member or CH inclines to leave the network or to join, a safe maintaining stage of the cluster is called for.

Nodes Clusters BN nodes

100 10 2

200 20 4

300 30 6

400 40 8

500 50 10

The concept of risk encompasses both external and internal attackers. The external attacker launches replay attack, black hole attack, Sybil attack, wormhole attack and targeted attacks. The RREQ package is one of the attacks to choose from. The internal attacker initiates a flood attack and play attack of Mov Conf during the maintenance phase of the cluster.

Simulation Parameters

Simulators NS2 version 2.32 is used to assess the SCSR proposed. The sink nodes are supposed to be located 100 meters from the above location. The imitation is carried out over 20 test runs for different scenarios and the average for each value is taken. As seen below, the simulation variables.

No. of Nodes is (n) 100 to 500Area Size is 500 × 500 m Routing protocol is CBDKT Simulation Time is 300 sec Traffic Source is CBR

Radio Propagation Model of Two-Ray Ground modelMAC IEEE 802.11

Antenna Type Omni Anenna

Mobility Model BN: No MobilityCH & SN: Random Method pointMobility Speed (m/s) 5

Pause time (sec) CH= 30, SN=10

Initial Energy (J) BN & CH=50, SN = 5Initial VBP (J) BN & CH=500, SN = 50

Reception power 0.0648W Transmission power 0.0744WIdle power 0.00000552W

No. of within Attackers 90% of attackers

No. of without Attackers 10% of attackersNo. of CHs is 10% of n

No. of BNs is 2% of n

5. Results and Discussions

In accordance with the EDDK system, the SCSR output is. The quality is measured mainly by the following measures.

Energy: It is the normal energy disbursed for the information transmission.

Network Resilience: Now we will quantify how attackers disturb the future of network resilience. It is determined by calculating the fraction of messages cooperated by collecting x-nodes among non-compromised nodes.

Packet Delivery Ratio (PDR): This reflects the proportion of the number of packets effectively delivered to the entirenumber of packets distributed and restrained when attacks take place.

No. of Alive Nodes: The remainder of the nodes remaining alive through the simulation rounds in the network is calculated.

Results

In a 500 node example, the numbers of attackers vary between 5,10,15,20 and 25. The figure displays the fraction of SCSR and EDDK methods ' compromised communications for various scenarios for the attackers. When the numbers of assailants are increased from five to 25, the number of attacks will increase as shown in the figure. Throughout intra- cluster and inter-cluster routing, SCSR recognizes malicious nodes and separates them from the network. We therefore can not engage further in the communications. Therefore, node capturing attacks will be challenging for the attackers.

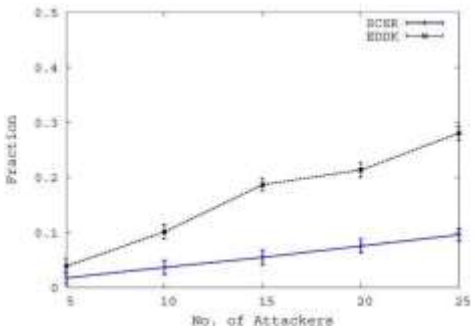

Figure VI.: Fraction of compromised communications by Attackers

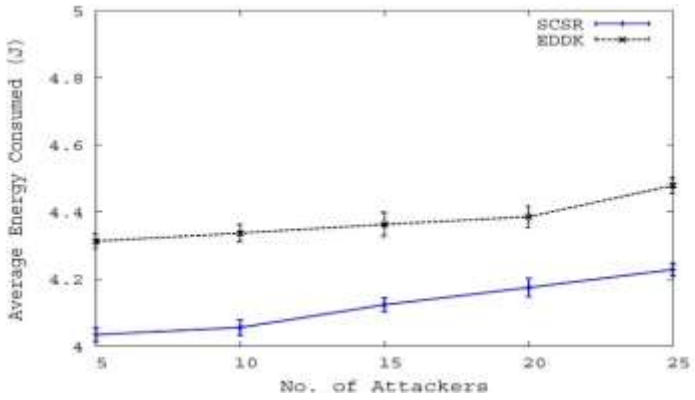

Figure VII. Average Energy Consumption in the presence of Attackers

The figure signifies the energy consumption for the various attacker situations for SCSR and EDDK techniques. Because EDDK frequently performs the local key and the cluster key, it uses further resources, while SCSR upgrades dynamically with less energy consumption.

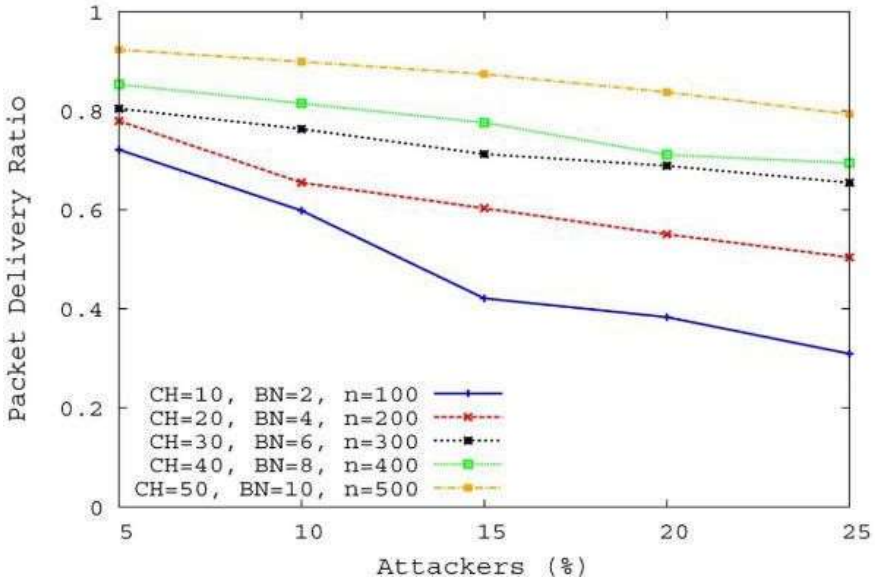

Figure VIII:Packet Delivery Ratio for SCSR

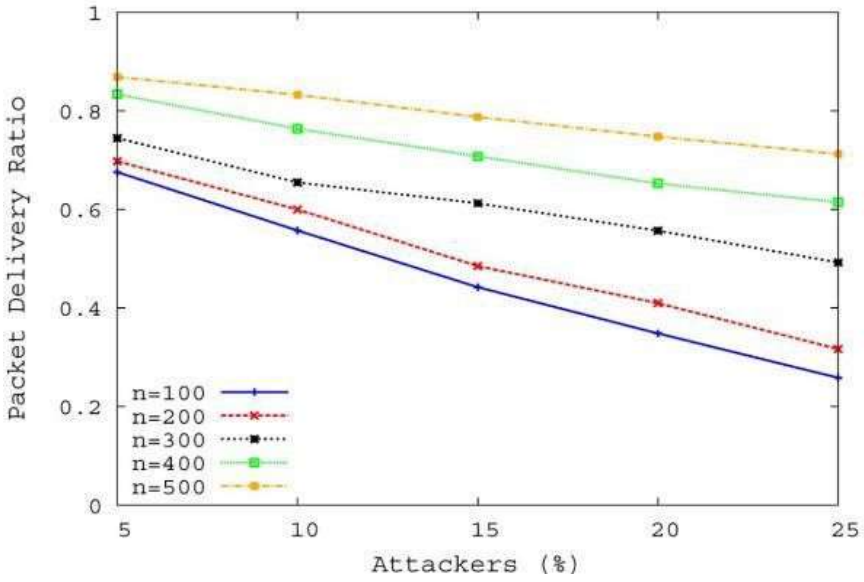

Figure IX: Packet Delivery Ratio for EDDK

The PDR for EDDK is shown in the figure. In this system the data can not be retrieved when one or several packets are attacked or discarded even if there are multiple paths entering the destination. This means that the PDR is less than the SCSR.

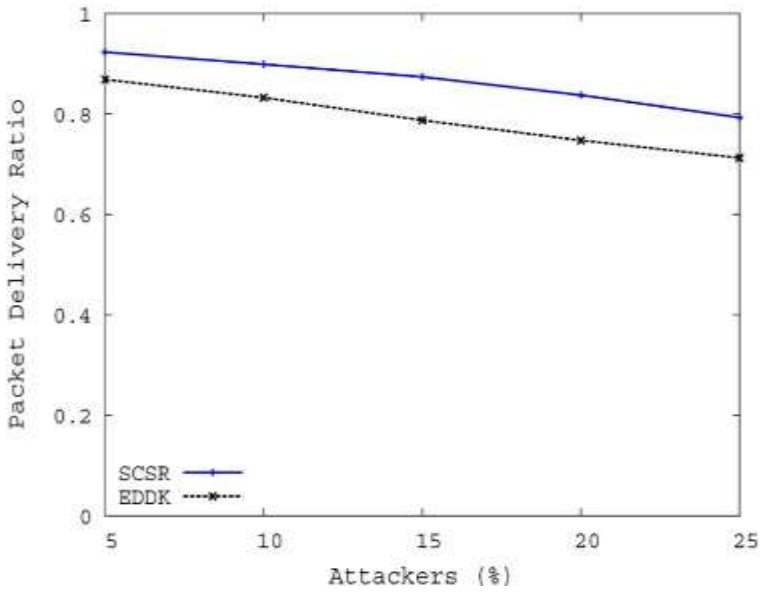

Figure X: Packet Delivery Ratio for SCSR and EDDK with 500 nodes

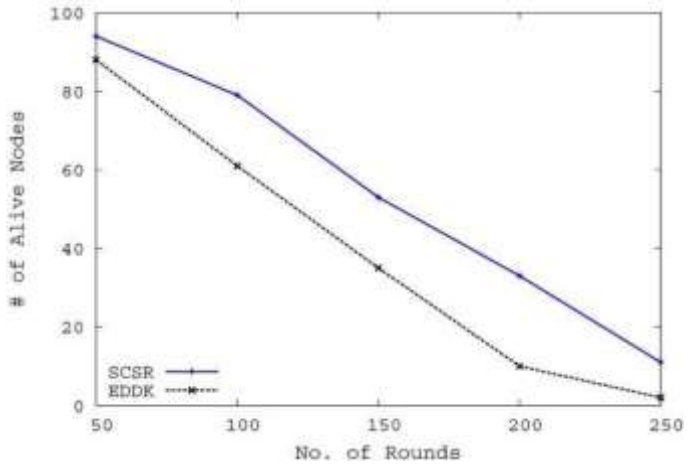

Figure XI: No. of Alive nodes v/s No. of Rounds

In contrast to dispersal technology, multipath routing is used in SCSR. With this dispersion process, the data is regenerated by the destination if minimum t shares between q shares directed by the origin are received. The flood messages from Mov Conf are filtered on the BN stage because they are not authenticated. The figure shows that, in contrast with EDDK, SCSR provides better PDRs. The number of living nodes for SCSR and EDDK methods for different execution rounds is shown in the figure. This indicates that the SCSR is more robust because at the end of 250 rounds, it has further alive nodes than EDDK. Because SCSR is less active in periodic main updates and cluster reconstructions, it uses less energy than EDDK.

6. Conclusion

In this research paper, the dynamic key administration technique SCSR for heterogeneous mobile wireless sensor networks is used. This security framework can be applied for medium and large scale applications that require security in all aspects. Includes the heterogeneous BNs used by the PSO technique in the network. Here, BN nodes use EBS to perform stable clustering. The cluster head will be selected based on the weight value determined with the aid of the ND, DBN, velocity and VBP parameters. Then, CCV values based on location, ND and VBP are determined by the cluster members. The dynamic keys are created by CCV, and then used to communicate intra-cluster information. The stable cluster maintenance is carried out when the node changes from cluster to cluster. When the data must be passed from source to sink, the clusters will perform secure route discovery. The simulated results show that in comparison with existing technologies SCSR consumes lower processing and requires minimal communication costs for sensor nodes. When comparison to the cost of the backbone nodes, the connectivity cost for the cluster heads is also smaller. The findings of the test show that the software introduced is safer and the overhead is minimized. Thus,SCSR provides a good packet distribution ratio because of the multi-dispersal routing technology and high security for intrusion attacks during data transmission.

References:

1. Abdelhakim, Mai, Lightfoot, Leonard E., Ren, Jian, and Li, Tongtong Distributed Detection in Mobile Access Wireless Sensor Networks Under Byzantine Attacks. *IEEE Transactions on Parallel And Distributed Systems*, **25** (4) (2013), 950 – 959.

2. Abduvaliev, Abror, Lee, Sungyoung, and Lee, Young-Koo, Simple hash based message authentication scheme for wireless sensor networks. In *9thInternational Symposium on Communications and Information Technology(ISCIT)* (2009), IEEE, 982 - 986.

3. Alrajeh, Nabil Ali, Khan, S., and Shams, Bilal, Intrusion Detection Systems in Wireless Sensor Networks: A Review. *International Journal of Distributed Sensor Networks*, **2013** (2013), 7 pages.

4. Amara, Said Ould, Beghdad, Rachid, and Oussalah, Mourad, Securing Wireless Sensor Networks: A Survey. *EDPACS: The EDP Audit, Control and Security Newsletter*, **47** (2) (March 06, 2013), 6-29.

5. Azarderskhsh, Reza and Reyhani-Masoleh, Arash, Secure Clustering and Symmetric Key Establishment in Heterogeneous Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking*, **2011** (2011), 12 pages.

6. Banihashemian, Saber and Bafghi, Abbas Ghaemi, A new key management scheme in heterogeneous wireless sensor networks. In *Advanced Communication Technology (ICACT), 2010 The 12thInternational Conference on* (Phoenix Park 2010), IEEE, 141 - 146.

7. Bao, Fenye, Chen, Ing-Ray, Chang, Moon Jeong, and Cho, Jin-Hee, *Hierarchical Trust Management for Wireless Sensor*

Networks and its Applications to TrustmBased Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9 (2) (IEEE Transactions on Networkmand Service Management), 169- 183.

8. Bellazreg, Ramzi and Boudriga, Noureddine, DynTunKey: a dynamic distributed group keytunneling management protocol for heterogeneous wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, **2014:9** (2014), 19 pages.

9. Boubiche, Djallel Eddine and Bilami, Azeddine, Cross Layer Intrusion Detection System For Wireless Sensor Network. *International Journal ofNetwork Security & Its Applications (IJNSA)*, **4** (2) (March 2012), 35-52.

10. Boujelben, M, Cheikhrouhou, O, Youssef, H, and Abid, M, A Pairing Identity based Key Management Protocol for Heterogeneous Wireless Sensor Networks. In *Network and Service Security, N2S '09. InternationalConference on* (Paris 2009), IEEE, 1-5.

11. Boulis, Athanassios, *Castalia: A simulator for Wireless Sensor Networks and Body Area Networks*. NICTA. 2011.

12. Braysy, V, Hurme, J, Teppo, H, Korpela, T, and Karjalainen, M, Movement tracking of sports team players with wireless sensor network. In *Ubiquitous Positioning Indoor Navigation and Location Based Service(UPINLBS), 2010* (Kirkkonummi 2010), IEEE,1-8.

13. Brownfield, Michael, Gupta, Yatharth, and Davis, Nathaniel, Wireless sensor network denial of sleep attack. In *Proceedings of the 2005 IEEEWorkshop on Information Assurance and Security United States MilitaryAcademy, West Point* (New York 2005), IEEE, 356- 364.

14. Chaaran, Khalid N, Younus, Munzza, and Javed, Muhammad Younus, NSN based Multi-Sink Minimum Delay Energy Efficient Routing in Wireless Sensor Networks. *European Journal of Scientific Research*, **41** (3) (2010), 399-411.

15. Chan, Haowen, Gligor, Virgil D., Perrig, Adrian, and Muralidharan, Gautam, On the Distribution and Revocation of Cryptographic Keys in Sensor Networks. *IEEE Transactions on Dependable and SecureComputing*, **2** (3) (2005), 233-247.

16. Chen, C.L and Li, C.T, Dynamic Session-Key Generation for Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking* (2008), 10 Pages.

17. Chen, Shuai, Liao, Xiaowei, Shu, Renyi, Shen, Xiaobo, Xu, Xiaojun, and Zheng, Xiaodong, Dynamic Key Management Scheme in Wireless Sensor Networks. In *High Performance Networking, Computing, and Communication Systems*. 2011.

18. Chen, Y and Yang, G, EBS-Based Collusion Resistant Group Key Management Using Attribute- Based Encryption. *China Communications*, **9** (1) (2012), 92-101.

19. Choi, Sung-Chan, Gong, Seong-Lyong, and Lee, Jang-Won, An average velocity- based routing protocol with low end-to-end delay for wireless sensor networks. *IEEE Communications letters*, **13** (8) (August 2009), 621–623.

20. Review of Security Attacks in Mobile Ad-Hoc Network, V Tulsyan , K Adhvaryu, TEST Engineering & Management, Scopus Indexed Journal, January – February 2020, ISSN: 0193-4120 Page No. 13832 – 13837.

21. Performance Comparison of Multicast Routing Protocols based on Route Discovery Process for MANET, K U Adhvaryu, Springer (Lecture Notes in Networks & Systems) International Conference on Innovative Communication and Computational Technologies (ICICCT -2019) during 29- 30 April 2019, Namakkal, India. Series ISSN: 2367-3370, eBook ISBN: 978-981-15-0146-3.

22. Energy Efficient ERS for Multicast Routing in MANET, K U Adhvaryu, IEEE International Conference on Recent Advances on Energy Efficient Computing and Communication (ICRAECC -2019) during 7-8 March 2019, Tamil Nadu, India.

23. Performance Comparison between Multicast Routing Protocols in MANET, K U Adhvaryu, P Kamboz, IEEE International Conference on Electrical, Computer and Electronics -2017 (UPCON 2017) on 26-28 October,2017 at GLA University, Mathura, IEEE Conference Record Number: 41590.

24. Survey of Various Energy Efficient Multicast Routing Protocols For MANET , K U Adhvaryu, P Kamboz, 5th International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom 2013, Bangalore published by IET- Elsevier.

25. Improved Route Discovery Technique for Multicast Routing in Mobile Ad hoc Network, K U Adhvaryu in International Journal of Emerging Technology and Innovative Research January 2015, Volume 2, Issue 1, ISSN: 2349-5162 (UGC approved Journal).