# Cross Layer Security Framework for Wireless Sensor Networks

Kalpana Sharma[1] and M.K. Ghose[2]
[1]Department of CSE, SMIT, Sikkim
kalpanaiitkgp@yahoo.com
[2] Department of CSE, SMIT, Sikkim
mkghose2000@gmail.com

***Abstract***

*Since the data collected by the nodes of WSN are sensitive and vulnerable to attack, there's a need of making the Wireless Sensor Networks (WSN) immune to attacks. Most of the researchers have come up with security solution to WSN based on layered approach. Layered approach has noticeable flaws like 'redundant' security or 'inflexible' security solutions. In this paper a new security scheme is proposed based on the concept of cross layer design methodology. Outline on the existing cross layer security schemes are also presented. The proposed approach doesn't claim to be immune to all the security attacks but this new approach certainly gives a new direction towards WSN security. The cross layer security framework has been tested with three important application types of WSN.*

***Keywords:*** *WSN, Layered security, Cross layer security*

## 1. Introduction

A wide variety of WSN applications like habitat monitoring, wildfire detection/monitoring, battlefield surveillances, military applications etc. are possible because of the development in WSN which consists of hundreds/thousands of nodes scattered in the area of interest to accomplish a particular mission. A lot of research is going on in the 'security' aspect of WSN. Most of the researchers are involved in the layered approach of security solution but very less attention is given in exploring the cross layer security solutions though both' layered and cross layer' fields have a lot of potential.

While designing the security mechanism for WSN it is to be kept in minds that the following are the inbuilt limitations of the sensor nodes. These are 1. limited computation capacity, 2. low battery life, 3. limited memory, 4. low bandwith,5. low communication range. So the cryptographic algorithms that are to be designed for WSN should not be 'overambitious' in the sense that security solutions meant for traditional networks cannot be applied , as such, for WSN security solutions.

Layered approach of security solutions tries to provide security either to all the layers which may be unnecessary or concentrate on just a single layer of the protocol stack. The following are the limitations of the layered security solutions.

1. Layered approach can provide security services for only one layer. Moreover some of these layered solutions address a particular kind of attack only. For example: providing security solution in link layer without securing the physical layer which results in a WSN with a weak security provision [4].

2. The above mentioned point doesn't mean that security is to be provided in each and every layer blindly. If is done do then such mechanism would drain out the WSN of all its limited resources like power, computation capacity, memory, battery life [16].

One of the common challenges of the WSN is the conservation of power, thus elongating the life span of a sensor node. A lot of research is being carried out towards 'energy efficiency' of WSN. Cross layer solutions for 'energy efficiency' is also being carried out in collaboration of physical layer, Network layer and link layer [4, 16]. It is seen that 'cross layer security solution' is still an unexplored field. In this paper an attempt has been made to secure the WSN with the help of 'Cross layer' approach. This work is an extended and enhanced version of [17]. The original format and the content of [17] are retained but all the sections have been enhanced and more in-depth analysis on security solutions have been incorporated.

An integrated security framework has been proposed by [13,14] in which the security solution provided is at par with the best and the authors have compared the results with TinySec[15] which is the de facto standard for the link layer security. In [14] though the security framework addresses all the concerns of WSN security goals, this solution is holistic, which means that security provisions prove to be' Overdone' if it is to be tried with various application domain of WSN. In other words when this security framework is to be used for different application scenario then apart from 'high security demanding' applications, the components has to reduce their 'Security' impact as per the security requirement, or else the security would prove to be inappropriate/ redundant for such application domain. For example the security requirement of 'Military application 'is quite different from that of 'Habitat monitoring' and 'Agricultural Farming'. In other words security concerns for a sensor networks and level of security desired may differ according to application specific needs, where the sensor networks are deployed. This paper proposes a security mechanism which is flexible and robust and it follows 'cross layer' approach of security.

Before discussing the components of the proposed Cross layer security solution, it is to be noted that various security applications have different security requirement. The sensor network security demanding applications of WSN are broadly divided into three broad categories. They are

- Hard security requirement applications (HSRA).
- Firm security requirement applications (FSRA).
- Soft security requirement applications (SSRA).

HSRA: Applications belonging to this category has stringent security requirements which cannot be compromised at all. All the security related parameters/attacks like confidentially, integrity, DoS, sibyl attack are to be carefully addressed. Compromise on any one of the security parameters would lead to a complete security failure of the network. Such applications cannot tolerate even a slighter degree of compromise on security parameters. HSRA has the lowest degree of tolerance to the security compromise. For example applications such as target tracking in a battlefield.

FSRA: Applications belonging to this category has a moderate level of security requirement and if not adhered to any one of the security parameters it doesn't lead to the complete security failure as in HSRA. Example in this category comprises of Habitat monitoring, Traffic monitoring etc. Such applications can tolerate a medium degree of security compromise.

SSRA: Applications belonging to this category has the lowest security requirement. Examples of SSRA are Environmental Monitoring (weather, temperature, and pressure), agricultural farming etc.

The security solution discussed in [13, 14] is for 'strict security demanding' applications i.e. HSRA. In order to make the security framework an' adaptive' to a specific application type, a new security solution is proposed in this paper which is an integrated comprehensive security framework that will provide security services for all services of the sensor network. This framework incorporates the flexibility to be 'application specific' security framework. This adaptive security solution is nothing but a 'Cross Layer Security Solution.' The 'Cross Layer Integrated Framework for Security for WSN (CLIFFs WSN or simply CLIFFs) includes the flavors of the 'Cross Layer Security Solution 'for WSN.

This paper discusses the salient features of the proposed 'CLIFFs'. CLIFFs provides security services to the WSN with the help of an added extra component called 'Intelligent Security Agent' i.e. ISA which is responsible for assessing the level of security and cross layer interactions. This framework supports many components like 'Intrusion Detection System', 'Trust Framework', 'and Key Management 'and' Link Layer Communication protocol'. ISA has been tested for three different application domains.

The rest of the paper is as follows. Section 2 deals with the background on some of the important security solutions, both cross layer oriented and layered oriented as cross layer technique is the extended version of the layered security solution approach. Section 3 deals with the proposed 'Cross layer Integrated Framework' in which all its components like key maintenance module, clustering module and link layer solutions are provided. Section 4 deals with the results followed by conclusion in section 5.

## 2. Literature Survey

In [2,3] it is noted that the protocol design for wireless sensor networks for reducing power consumption cannot be handled completely in one layer of the protocol stack. So here the importance of cross layer interaction is realized. In paper [1] a CSMA/CA sleep/wake MAC protocol is proposed that minimizes internode interference, while also reduces per-hop delay through cross-layer interactions with the network layer. The] suboptimal algorithm [1] is based on a cross-layer approach in the way of collecting the corresponding information from the PHY and MAC layers. In some of recent works, there are cross layer implementation for power management schemes, path redundancy based security [9].

Bhaskaran Raman et al. [5] pointed out that WSN protocols are very deeply dependent on application scenarios, but most of protocols does not cite or use any specific application in its design. So current security schemes also lacks in providing security to specific scenarios while assessing their security needs. There are some approaches which addresses only routing problem like Secure SPIN, Secure Sensor Network Routing and some other geographic techniques. Tae Kyung Kim et al. [6] give a simple trust model using fuzzy logic that addresses the secure routing problem. It calculates the evaluation value for each path and ensures that packet is always forwarded to a high evaluation value path. A scheme for preventing compromised node to become cluster head is proposed by Garth et al. [10] which is based on trust factor and some initiatives to provide security framework, which integrates two or more security schemes like secure cluster formation key management etc. It supports holistic security approach to provide security to WSNs. But major disadvantage of holistic security approach is that it tries to implement security layer wise which results in redundant security.

Currently much of work is going on providing layered security for example in Holistic Security Approach [7]. A holistic approach aims at improving performance, security, longevity with respect to changing environmental condition with some basic principles like, in a given network security is to be ensured for all the layers of the protocol stack and also the cost of security should not be more than assessed security risks. But the major disadvantage with holistic security is that it is layered and tries to implement security mechanisms for each layer, which results in wastage of power, memory, processing power and introduce message delay.

## 3. Proposed 'Cross layer Integrated Framework For security' for WSN (CLIFFs)

There are various WSN applications (military, health, etc.), as already pointed out in section 1, that require a strong level of Security. In order to provide a flexible security solution platform a few reasonable assumptions are made the first assumption being 'the Base Station (BS) is safe and adversaries cannot compromise it'.

### 3.1 Design Guidelines

In order to realize a 'cross layer security solution' for a practical security framework in sensor networks the following design guidelines are adhered to, which are as follows:

1. Component Based Security:-Some kind of security measures must be provided to all the components of a system as well as to the network as a whole .The designer should concentrate on securing the whole network
2. Robust, simple and flexible Designs: - Security design should build trustworthy system out of untrustworthy components and should have ability to detect and function when need arises. Security framework should also work if we add new nodes in the network thus providing scalability
3. Adaptive Security:-WSNs have numerous combinations of sensing, communication and computing technologies and sensors are deployed from very sparse to dense in quantities. So depending on traffic characteristics and environment they have to adapt themselves. For example - in a good environment where probability of security attacks is low, low level of security should be used i.e. the application should be considered as of SSRN group. In other words, the sensor network should adapt them according to the outside environment. The notion of adaptive security is further categorized into following sub-categories.
    - Application based: - As already described in previous section that each application requires different level of security. The goal of this proposed framework is 'the development of application specific security framework'.
    - Data Based: - Level of security also depends on the type of data. For example there should be different level of encryption for routing, sensed data, control packet data and encryption key information.

There are other categories of ' Adaptive Security' but in this paper two components i.e.' application based' and 'data based' are highlighted.

The proposed 'CLIFFs' is based on the following security recommendations.

1. If the routing should be energy efficient then during routing algorithm design it is to be seen that the minimization of the control packets is done (Network layer), retransmission (link layer) is to be reduced and energy transceivers are put in On/Off state in physical layer. This shows that there should be an interaction between all these layers.

2. Key management schemes make sure that all the communicating nodes possess required keys for encrypted communication, at the same time to make sure that packet reaches destination, a secure link with multi path routing is required.

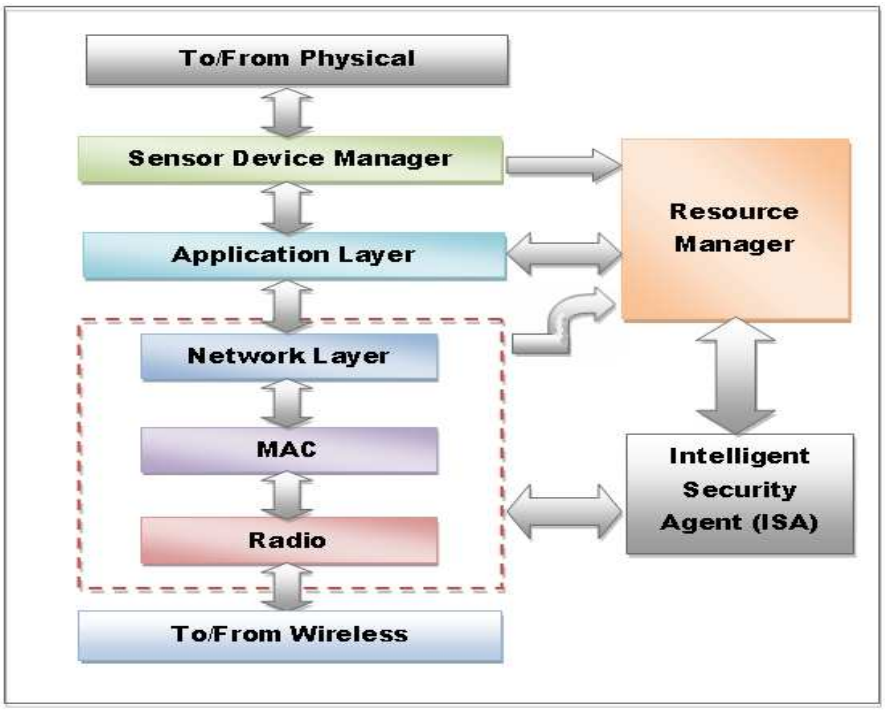


**Figure 1: ISA and its coupling with the protocol layers**

To reduce the overhead created by cross layered architectures, an Intelligent Security Agent (ISA) is introduced to follow guidelines given in Subsection 3.1 and to provide energy efficient and non redundant security operation while keeping protocol layer abstraction. ISA will be used as a separate component in the node architecture as shown in figure 1.ISA exchanges parameters with all protocol layers and acts like a Resource Manager.

To be a part of a component based security framework, security is to be ensured for all the components in a system and services. To achieve this goal the proposed CLIFFs consists of the following components as its main building blocks. These are Trust Framework using Cross Layer Approach, Trust Based Group Head Election, Key Management Architecture and Adaptive Secure Communication Protocol.

### 3.2. Cluster Formation based on Trust Framework

In order to establish a communication and sustain it the WSN should have a topology. The topology considered in this paper is 'hierarchical clustering' as it is very practical one. A hierarchical approach breaks the network into cluster layers. Nodes are grouped into clusters under the leadership of a Cluster Head (CH) which has responsibility of routing data from the clusters to the other CH or Base Station (BS). Data travel from a lower CH to the higher level CH and finally to the BS. More on clustering techniques can be referred from [11].The following assumptions are made before discussing the cluster formation technique used in CLIFFs.

#### 3.2.1 Assumptions

- Location of each node is known to the BS.
- Time Division multiplexing (TDM) is used for communication in a group, in which for a particular interval, a node will transmit otherwise It will listen passively in promiscuous node. So a node can hear neighborhood transmission/reception.
- The BS is very powerful with a huge computational capability.

Before any transmission takes place, all the nodes have to register themselves with the BS. Each node in a network is identified by a set of Group id (8 Bits) and Node id (8 Bits) i.e. {Groupid, Nodeid}.So node communication is limited to group only.The sensor nodes use a battery that has a limited power source. So when these nodes are in function, their energy level goes lower and lower. To optimize this, when the nodes are not doing either computational work or transmission work or sensing work, they go to sleep state. They become active only when they have some message of interest to send to their respective cluster head. The node sends its data without fail if its power value is above a pre set threshold value. In CLIFFs this threshold value is set to be 20% of the total battery power. As the energy meter of the node shows that the power has fallen below this value, the node comes to know that it is going to die out soon. This gives rise to two different situations in the network, either a cluster head falling short of power Or An ordinary node falling short of power.The case of CH's depleting energy is of utmost importance due to the reason that this node has some extra assigned responsibility of data aggregation which is not there for other nodes. In other words to maximize the network life time, a node with highest energy is chosen to be group head/ CH. Since a CH has to perform one of the most important operations i.e. data aggregation the rate of consumption of power is very high in case of CH. So the role of CH should be rotational to conserve energy and when a node falls short of energy, it will transfer its responsibility to some other node in group by election or some other measures. Let available energy be the parameter which determines which node will be the CH and to transfer group head responsibility. A compromised node or an adversary always shows higher amount of energy, so there is a high probability of selecting an adversary as a CH. Most of current clustering techniques assume that all the nodes are trustworthy in a network. A technique is to be devised in which the probability of selection of compromised nodes as CH is very low.

Figure 2 shows a situation in which CH is ready to shed off its responsibility as CH as it has almost exhausted its battery life.

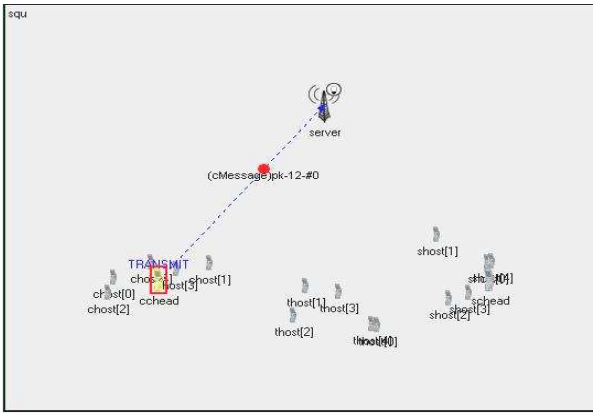


**Figure 2: CH broadcasting for re-election.**

In CLIFFs a node continuously monitors its neighbors and maintains a parameter table. All the parameters values are collected from cross layer interactions. The parameters which are

considered for choosing the CH are shown in table 1. Depending on these parameters all the nodes of the Trust Framework compute a trust level of all its neighbors. The parameters used are summarized in table 1.

**Table 1: Parameters for trust calculation**

| Sl. No | Parameters | Node1 | Node2 | Node m |
|---|---|---|---|---|
| 1. | Available Energy (AE) | | | |
| 2. | Packet Signal Strength (PSS) | | | |
| 3. | Control Packet Received for forward(CRF) | | | |
| 4. | Control Packet Received forwarded(CRAF) | | | |
| 5. | Routing Cost (RC) | | | |
| 6. | No. of Packet Collision (NPC) | | | |
| 7. | Data Packet Received for forward (DRF) | | | |
| 8. | Data Packet Received forwarded (DRAF) | | | |
| 9. | Packet Dropped (PD) | | | |
| 10. | No. of Packets Transmitted (NPT) | | | |
| 11. | No. of Packets Received (NPR) | | | |

CRFi - Control Packet Received for forward for a particular node i. where i=1, 2… m. same notations apply to CRAF, DRF, DRAF, NPT, and NPR.
AEi (T1) – Available Energy for a node i at a time T1.Same notations also apply for PSS and RC.
Now we will calculate trust values are calculated from these parameters which are shown in table 2.

Trust based cluster scheme described above is motivated by [10]. Not all the parameters mentioned in [10] are used as some extra parameters are included as well as some parameters are discarded while calculating trust value to make the proposed scheme more generalized and robust. After computing trust level of each neighbor, a node will use these values during routing phase also. Steps for choosing CH are as follows

- Step-1. Whenever a CH finds that, it is unable to bear the CH responsibility due to some reasons like low energy etc it broadcasts a message for re-election.
- Step-2. If a node gets election message, then it will find a neighbor with highest trust value and send this to the current CH as a vote.
- Step-3. Now, CH will assign this responsibility to the node, which has highest number of votes. Ids of CH and will be directly broadcasted to all group members using a secret key i.e. buddy key (Kb). Details on the key are discussed in section 3.3. All communication described above must be encrypted using appropriate keys as described in next section.

**Table 2: Calculation of the Trust parameters (P)**

| |
|---|
| P1 = (AEi (T1) - AEi (T2)) / AEi (T1) where T1 < T2. |
| P2 = (PSSi (T1) - PSSi (T2)) / PSSi (T1) where T1 < T2. |
| P3 = CRAFi / CRFi. |
| P4 = DRAFi / DRFi. |
| P5 = 1 - NPCi / NPTi. |
| P6 = 1 - PDi/ NPRi. |

Here Ti= Trust Level of Node i, calculated by node, which is maintaining above table.

$Ti=w1* P1 + w2* P2 + w3*P3 + w4* P4 + w5* P5 + w6*P6.$

Here w1, w2, w3, w4, w5, w6 are constants, whose value is chosen such that $Ti < 1$.

### 3.3 Key Management Architecture

There is a very practical key management scheme proposed by Hamed et al. [12] which provides a strong defense to node compromised attacks. But a major drawback of this scheme is it does not provide any mechanism for changing keys periodically, as it derives all the required keys from the key given before deployment. In this paper a keying technique is proposed which considers the periodic refreshment of keys. The following keys are used in the proposed framework.

- Buddy key (Kb) is calculated by all the nodes once the neighbors finding work is over. It is used to communicate by each node within its own group/cluster.
- My-Own-Key (Ko) is used by each and every node initially. All the nodes are preloaded with its id and this key is a function of node id, group-id and its residual energy.
- Network key ( Kn) is issued by the BS after authentication to all the nodes. If a node joins the network it has to send a request to BS for acquiring network key. This request is sent by all the nodes to the BS encrypting it by Ko. BS sends the 'Kn' to the requesting nodes encrypting it with 'Ko' of that particular node. Only the node which is authentic can decrypt this 'Kn'.
- Broadcast Key (Kbro) is issued by the BS after authentication as CHs.This is usd for CH to BS communication.

In [14] the keys are predeployed but in this scheme only node-id is preloaded and Ko is calculated in the network itself which means it is a in-network key. Buddy key is also calculated between neighbors. Only Kn and Kbro are communicated by BS. Most of the keys in this protocol are in-network calculated as 'computation is cheaper than communication' in WSN and safer than that of predeployed keys.

### 3.4 Adaptive Secure Communication Protocol

Link layer security protocols proposed till date donot provide adaptive security. So an adaptive security protocol is proposed in this paper, which dynamically adjusts itself to a particular security level depending on the network state. Mechanism of providing adaptive security is handled by a component ISA (Intelligent Security Agent), which is used to make cross layer interactions easier.

The packet format considered can be shown as follows. All the values are in bytes. Table 3 shows the packet format for TinySec-Auth+ Encryption [15] and table 4 shows the packet format for the proposed framework.

**Table 3: TinySec packet format**

| Dest | A | L | Src | ctr | Data | MAC |
|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 2 | 2 | 0-----29 | 4 |

**Table 4: CLIFFs packet format**

| D | A | L | G | Src | ctr | Data | MAC |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 0-----29 | 4 |

In the packet format used for CLIFFs group field is introduced because use of group field is crucial because in CLIFFs the whole network is divided into groups and the nodes communicate with the group members only. Here group field is of 1 byte which results in a network which can support 256 different groups, and using source id and destination id of 1 byte, a group can support 256 different nodes. So in this scheme the number of nodes that a network can support is 256*256=65536 nodes, which is same as that of Tinysec. Packet overhead due to source and destination id in Tinysec is of 2+2=4 bytes. But in this scheme it is 3 bytes (including group field).Because a node can be distinguished by using {Groupid , Sourceid} or {Groupid, Destinationid}.This is agreement with the previous assumption that communication of a node is limited to its group members only. Maximal payload length in Tinysec packet can be of 29bytes .But payload length cannot be greater than 5 bits and MSB 3bits are unused in each data packet sent. This unused 3 bits MSB is utilized for providing adaptive security in CLIFFs. First 2 bits will be used for encryption level and third bit will be used for authentication purpose.

**Table 5: Different Level of Encryption**

| Bits Rep | Level | Operation | Example | Application type |
|---|---|---|---|---|
| 00 | Level -0 | Simple XOR | Agricultural farming | SSRA |
| 01 | Level-1 | RC5/80/4 | Habitat Monitoring | FSRA |
| 10 | Level-2 | RC5/80/8 | Environment data collection | HSRA/FSRA |
| 11 | Level-3 | RC5/80/12 | Battlefield Surveillance | HSRA |

Here RC5/80/4 represents RC5 encryption algorithm with key size 80 bits and encryption rounds 4.

Different encryption levels are shown in table 5. RC5 encryption is used as a block cipher and MAC is used for authentication. Four level of encryption is used to provide adaptive security. Level of encryption will be provided by ISA.

## 4. Results and Discussion

For implementation of CLIFFs, Castalia simulator based on Omnet++ is used by adding ISA. The approach proposed in this paper stresses on group communication and diversity of application scenarios, so it has been tested it on three different application scenarios i.e. 'Military Surveillance System', 'Habitat Monitoring' and 'Agricultural Farming each representing HSRA, FSRA and SSRA respectively as mentioned in section 1 and shown in figure 3.

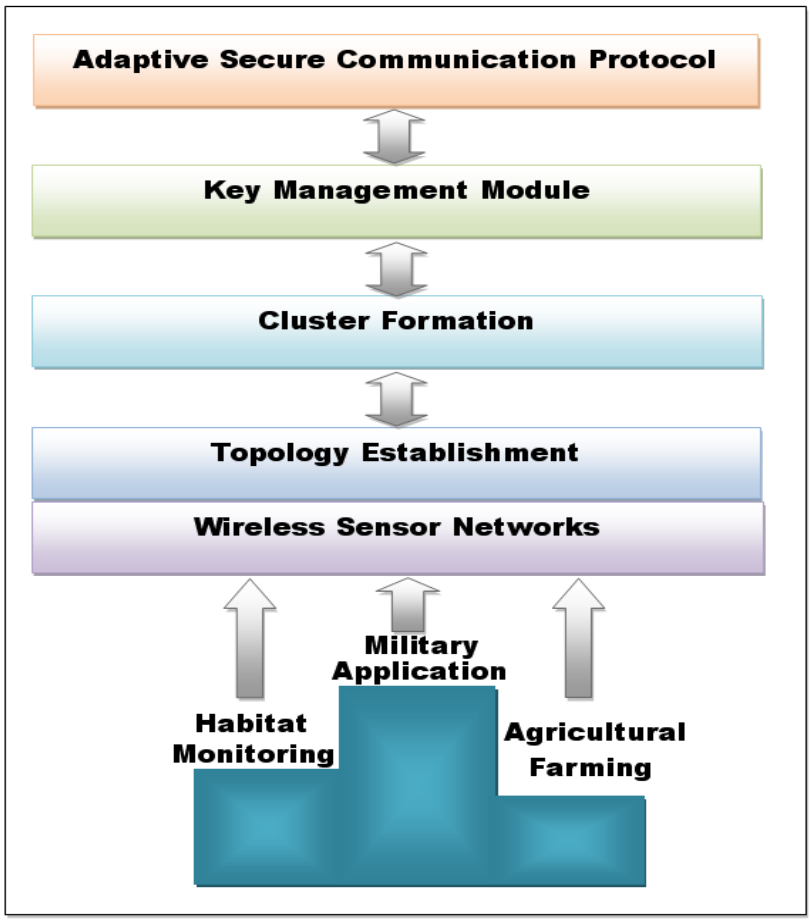


**Figure 3: Various application scenario being handled by the CLIFFs.**

These three different application scenarios correspond to high, medium and low level security respectively. Table 5 provides the different security requirements of these scenarios. A comparison is done between using fixed security level and variable security level as shown in figure 4-6.

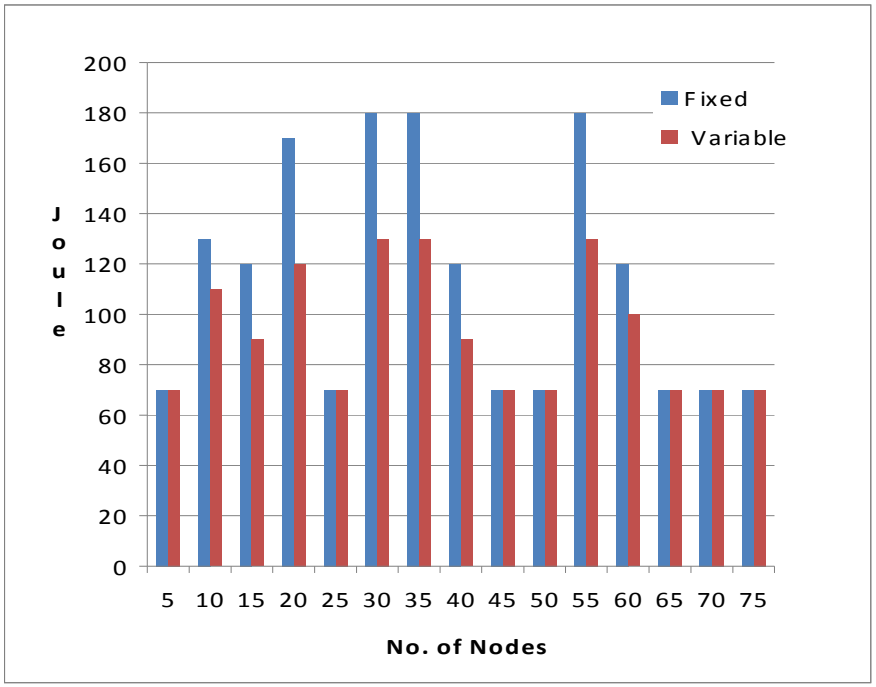


**Figure 4: Comparison of results for HSRA with / without ISA**

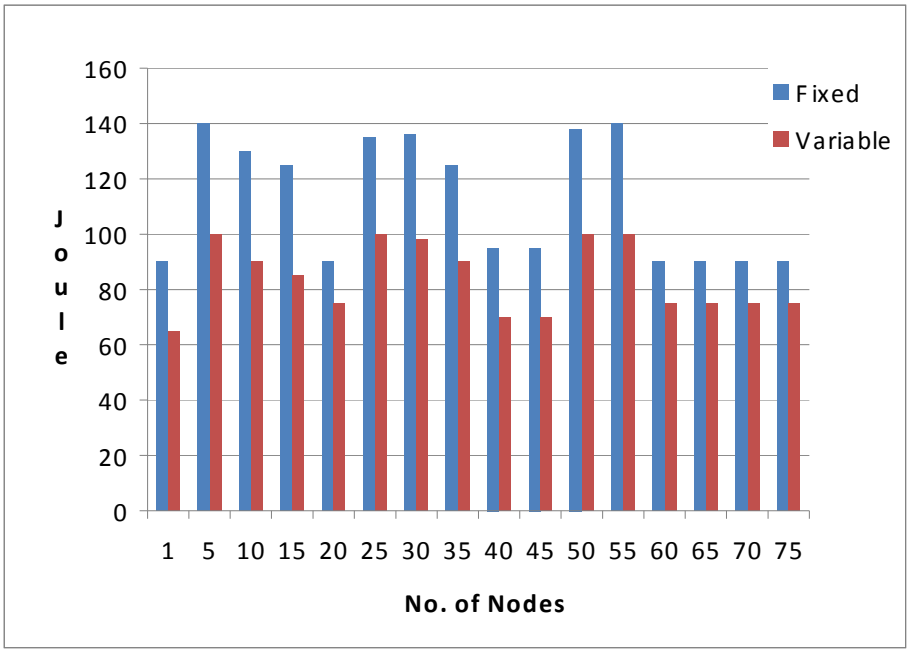


**Figure 5: Comparison of results for FSRA with / without ISA**

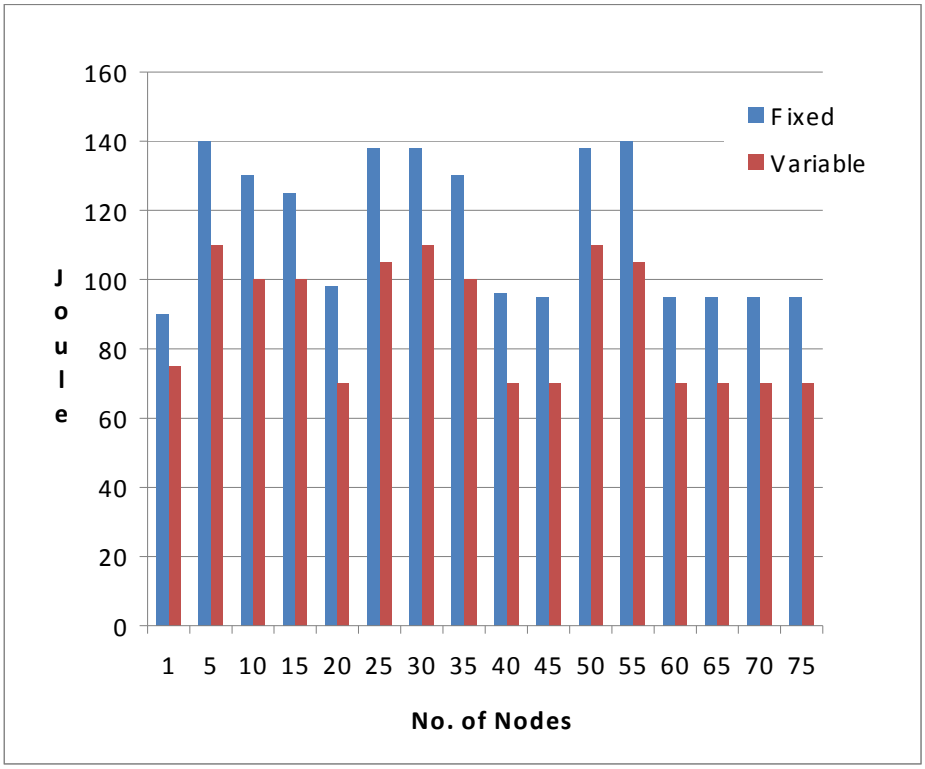


**Figure 6: Comparison of results for SSRA with / without ISA**

In the figures (4-6), the x-axis represents the number of nodes and the y-axis represents the energy in Joules. It can be seen from the results that that the function of ISA is prominent in case where the level of security to be achieved is known in advance like in case of 'Military application' the level of security is very high, thus the use of ISA is immaterial in this case as there will be very low energy saving whereas in case of 'Agricultural Farming' ISA plays an important role thus the amount of energy saved is very high. In case of "Habitat Monitoring" energy saved is moderate.

Use of ISA results in energy saving and is achieved by variable encryption level in adaptive link layer protocol. Depending on current percept ISA will determine an adaptive reaction for level of security that would incorporate many policies and recommendations which can also be given at the time of deployment or afterwards. Here percept information is collected from various layers using cross layer interactions and from resource Manger. Percept Information may include following information

- Type of Information.
- Available Memory at that time.
- Available Energy.
- Trust Level of Neighboring Nodes.
- Predefined Policies and Recommendations.

ISA will maintain a decision binary tree, which must be updated from time to time using new inputs. Two sample decision binary trees has been shown in figure 7 & 8 for better understanding .However functioning of ISA largely depends upon the correct predefined policies and

recommendations, for example if the network being used is in agricultural specific scenario then it must be specified during the time of deployment so that ISA can adjust itself to the security level appropriate for that application.

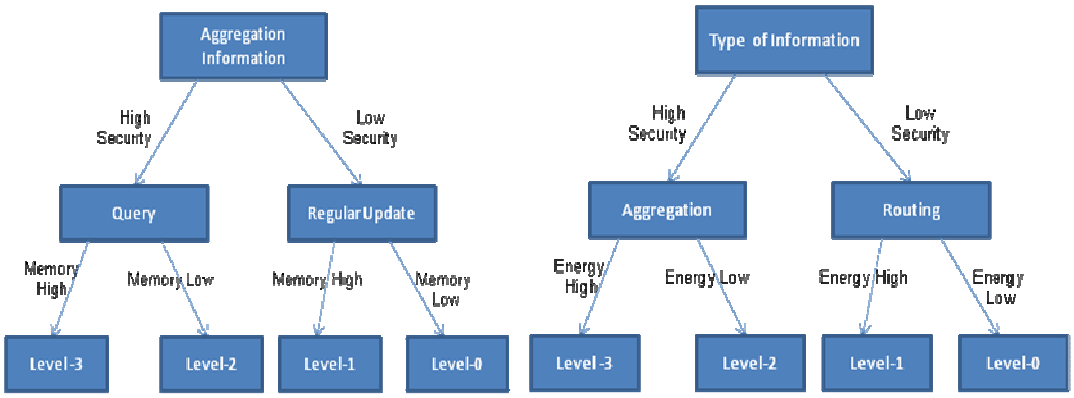


**Fig 7, 8 - Sample Decision Binary Tree used by ISA**

## 5. Conclusion:

In this paper a new approach of security soltion for WSN is presented. The proposed security framework CLIFFs, with the help of ISA, is used as an adaptive security solution for different application scenerio.The results obtained showed that CLIFFs, when provided with the right information regarding the application type, resulted in saving of energy to a large extent.

There's a lot of scope of improvement for CLIFFs. ISA can be used to incorporate the concept of 'learning' during its phases of execution. A robust security can be realized if ISA, on itself, decide upon the level of security based on the deployment history of the WSN.CLIFFs can be further enhanced if it is encorporated with highly accepted ' Energy Effieient Routing Protocols ' and 'Keying techniques' etc.

**Acknowledgment:** The authors would like to acknowledge the efforts of Kuldeep Yadav, an ex-student of CSE Department, SMIT, Majitar, Sikkim, India. His contribution for the work presented in this paper is highly acknowledged.

## 6. References

1.T. Melodia, M. C. Vuran, and D. Pompili, "The state of the art in cross-layer design for wireless sensor networks," Proceedings of Euro-NGI Workshops on Wireless and Mobility, Springer Lecture Notes on Computer Science, LNCS 388, Como, Italy: 2005.

2. V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead," Communications Magazine, IEEE, vol. 43, 2005, p. 112,119.

3. M. Sichitiu, 'Cross-layer scheduling for power efficiency in wireless sensor networks', IEEE INFOCOM 2004, pp. 1740-1750.

4.. Ayman Khalil, Matthieu Crussière and Jean-François Hélard,'Cross Layer Resource Allocation Scheme under Heterogeneous constraints for Next Generation High Rate WPAN (2010),International Journal of Computer Networks and Communications( IJCNC) vol 2, No. 3.

5. Bhaskaran Raman et. al, Censor Networks: A Critique of "Sensor Networks" from a Systems Perspective, ACM SIGCOMM Computer Communication Review, Volume 38, Number 3, July 2008

6. Tae Kyung Kim, and Hee Suk Seo, A Trust Model using Fuzzy Logic in Wireless Sensor Network, Proceedings of world academy of science, engineering and technology volume 32,August 2008.

7. Al-Sakib Khan Pathan et. al. "Security in Wireless Sensor Networks: Issues and Challenges" in Feb. 20-22, 2006, ICACT2006, ISBN 89-5519-129-4 pp(1043-1048).

9. Sami S., Wakeel and Eng. Saad A. AL-Swailem,"PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks", WCNC 2007 Proceedings, pp(4159-4163).

10 Garth V. Crosby, Niki Pissinou, James Gadze, A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks, Proceedings of the Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS'06).

11 Jamil Ibriq, Imad Mahgoub, Cluster-Based Routing in Wireless Sensor Networks: Issues and Challenges.SPECTS'04, ISBN: 1-56555-284-9:759-769, California.

12 Hamed Soroush, Mastooreh Salajegheh and Tassos Dimitriou, Providing Transparent Security Services to Sensor Networks. In Proceedings of IEEE International Conference on Communication (ICC'07).24-28 June 2007.

13 T.A Zia and A.Y. Zomaya, 'A Secur Triple-Key Management Scheme for wireless sensor networks', in the proceedings of INFOCOM 2006,25th IEEE International Conference on Computer Communications, Barcelona, pp1-2 ,23-29 April 2006.

14 Tanveer Zia and Albert Zomaya," A Security Framework for Wireless Sensor Networks ", SAS 2006 – IEEE Sensors Applications Symposium Houston, Texas USA, 7-9 February 2006.

15 C. karlof, N. Shastry and D. Wagner, TinySec: link layer security architecture for wireless sensor networks, SenSys'04, November 3-5, 2004, Baltimore, Maryland, USA.

16 Mingbo Xiao,Xudong Wang,Guangsong Yang,'Cross-Layer Design for the Security of Wireless Sensor Networks', Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China.

17 Kalpana Sharma, M.K. Ghose, Kuldeep, 'Complete Security Framework for Wireless Sensor Networks', International Journal of Computer Science and Information Security, IJCSIS July 2009, Vol. 3 No. 1, USA.

## Authors

1. Mrs Kalpana Sharma : Mrs Kalpana Sharma is an Associate Professor of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Mazitar, Sikkim, India since August, 1998. She did her BE from National Institute of Technology, Silchar, India and M.Tech from IIT Kharagpur, India.Her areas of research interest are Wireless Sensor Networks, Steganography, Network & Information Security, Real Time Systems and Software Engineering. She has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international/ national conferences. She can be reached at kalpanaiitkgp@yahoo.com.

2. Prof (Dr.) M.K. Ghose: Dr. M.K.Ghose is the Professor and Head of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Mazitar, Sikkim, Indi SINCE June, 2006. Prior to this, Dr. Ghose worked in the internationally reputed R & D organisation ISRO – during 1981 to 1994 at Vikram Sarabhai Space Centre, ISRO, Trivandrum in the areas of Mission simulation and Quality & Reliability Analysis of ISRO Launch vehicles and Satellite systems and during 1995 to 2006 at Regional Remote Sensing Service Centre, ISRO, IIT Campus, Kharagpur in the areas of RS & GIS techniques for the natural resources management. He also associated with [Regional Engg. College ( NIT ), Silchar (1979 – 1981) as Teaching Asst. and Assam Central University, Silchar as COE and HOD of Computer Science Department (1997-2000).His areas of research interest are Data Mining, Simulation & Modeling, Network & Information Security, Optimization & Genetic Algorithm, Digital Image processing, Remote Sensing & GIS and Software Engineering. Chaired a number of international/national conference sessions. Dr. Ghose has conducted quite a number of Seminars, Workshop and Training programmes in the above areas and published 100 technical papers in various national and international journals in addition to presentation/ publication in several international/ national conferences. Presently 9 scholars are pursuing Ph.D work under his guidance and he is having 8 sponsored projects worth of 1 crore. Dr Ghose also served as technical consultant to various reputed organizations like IIT, Chennai, IIT Kharagpur, WRI, Tricy, SCIMST, KELTRON, HLL, Trivandrum. He can be reached at headcse.smit@gmail.com.