New Framework for Enhanced Secure Key Management in Hierarchical Wireless Sensor Network

Avant Panwar
Department of Computer Science Engineering
Delhi Technological University
New Delhi

Manoj Kumar
Department of Computer Science Engineering
Delhi Technological University
New Delhi

Sajendra Kumar
Department of Computer Science Engineering
IIMT Institute of Engineering and Technology, Meerut

ABSTRACT
The salient features of WSN like use of wireless radio communication, collaborative nature and deployment in the open environment exposes it to many security threats. Since WSN has tight limitations on the power consumption, transmission and computation the complex cryptographic algorithms can't be used to provide the security. Key management in WSN is the fundamental line of defense for a secure communication and thus it is very important. In this paper we propose a new framework for enhanced key management for hierarchical WSN which enhances the security of the network. In the proposed framework the base station computes all the keys required for both inter and intra cluster communications. Cluster is further isolated into small geographical areas on the basis of hop count from the cluster head. The sensor nodes in the network join the cluster on the basis of the distance (hop counts) from the cluster head which localizes the path key things and reduces the overhead. The proposed framework is divided into four stages pre key distribution, pair wise key establishment, computing the path key and re keying all the keys.

General Terms
Wireless sensor network, security, key management, hop count, and cluster.

1. INTRODUCTION
The WSN consists of large number of tiny sensor nodes which have restricted/limited battery life, communication bandwidth, storage capacity ,computation capabilities and open wireless communication channel .These constraints on the WSN arises many security threats (and issues like network access control, authentication, confidentiality and compromising nodes) for which security in the WSN is required. In WSN cryptography is used to provide the data confidentiality, integrity and authentication so in order to use it effectively the cryptographic keys are to be exchanged and that's where the efficient key management comes into play. Key management is one of the most important and basic aspect of WSN which provides the base for the various other secure mechanism like secure routing , secure localization etc
Security in WSN has six challenges wireless nature of communication,

1. resource limitation on sensor nodes
2. very large and dense WSN
3. lack of fixed infrastructure
4. unknown network topology prior to deployment
5. high risk of physical attacks to unattended sensors.

Moreover, in some deployment scenarios sensor nodes need to operate under adversarial condition. Security solutions for such applications depend on existence of strong and efficient key distribution mechanisms. It is infeasible, or even impossible in uncontrolled environments, to visit large number of sensor nodes, and change their configuration. Moreover, use of a single shared key in whole WSN is not a good idea because an adversary can easily obtain the key. Thus, sensor nodes have to adapt their environments, and establish a secure network by:

1. Using pre-distributed keys or keying materials.
2. Exchanging information with their immediate neighbors.
3. Exchanging in-formation with computationally robust nodes.

Key distribution and management problem in WSN is difficult one, and requires new approaches. A lot of work had been done in the field of key management but Eschenauer and Gligor[1] were the first one to address the key distribution problem in WSN. In their approach they made a universal key pool and every node in the network was given a predefined number of keys by uniformly randomly choosing keys from the pool. The keys are then deployed in the node (chosen for each node) which constitutes its key ring. All the nodes are then randomly deployed in the field and secure communication link is established by discovering the common keys among the neighbors i.e. each node in network share its key ring to discover at least one common key for communicating with the neighbor over a secure link. The main problem with this scheme is that it fails to provide sufficient security when there is an increase in the number of compromised nodes in the network. Since sensor node has low cost, non tamper resistant hardware so if a node gets compromised all the stored information can be extracted out of it by the adversary. To enhance the network resilience against node capture attacks, Chan et al.[2] devised a approach which further extended this idea and proposed the q-composite key pre-distribution Approach which allows two sensors node to setup a pair-wise key only when they share at least q common keys. Chan et al. also developed a random pair-wise keys scheme to defeat node capture attacks. Various other schemes were proposed for the key management which were the extension of these ideas only Zhu et al. [3] give Localized Encryption and Authentication Protocol (LEAP), a proposed scheme based on local distribution of keys among nodes in a neighborhood.

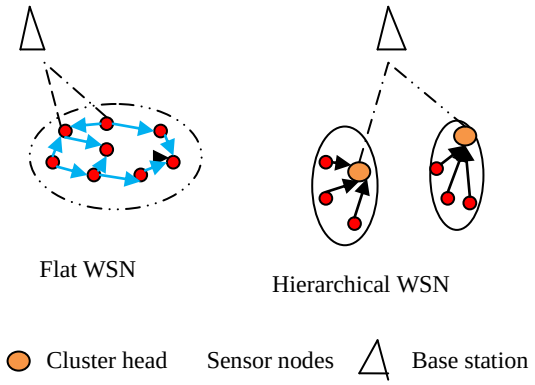

Figure1: Wireless Sensor Network Architecture

2. Related Work

Various work have been proposed so far in the field of key management with many of them focusing on the random key distribution among the nodes in the network [1]Chan et al [2]the q-composite key pre-distribution, Zhu et al. [3] give Localized Encryption and Authentication Protocol(LEAP) Other schemes based on the distance were also proposed for the key management[4,5,6,7].

The RKPH[4] scheme is based on Random key distribution and uses different keys in different clusters and takes distance of sensor node from their cluster head into account. It preloads some base keys into sensor and the new keys are derived by considering the distance of sensor node from their cluster head and to which cluster does the sensor node belongs. The main problem with this scheme was that it uses the two different types of sensor nodes H-sensors and L sensor where H sensors have high battery, storage and computation power while the L sensors have the usual restrictions. These nodes increase the cost of the network and drive the approach away from the practicality. Another similar approach HKMS[6] and DKM[5] was proposed which localizes the key thing by counting the number of hops i.e. distances of sensor node from its cluster head. It divides the cluster into different level on the basis of the distance (hop count) and provides the different keys for different levels. The main problem with these approaches is that they didn't provided sufficient security for the intra cluster communication .Other scheme ESKMS[8] which uses the simple encryption and one way hash function to distribute the keys among the nodes in the network and provide a unique key for communication between the nodes in the network.

3. Network Model

In our network model we considered the following:

- The BS is a control center and connects the WSN with external network for processing of the sensed data. Further, it is assumed that the base station has unlimited computational, communication, and memory resources and it is considered trustworthy and it can also transmit directly to every sensor node.
- Sensors nodes collect information of surrounding environment and transmit them to their respective cluster head.
- Cluster heads are responsible for the coordination, the data retransfer and the management of all the nodes in the cluster.
- We assume that WSNs are homogeneous and symmetric. Nodes are deployed randomly in the network.
- Sensor nodes keep stationary after deployment during the network operation.
- All the sensor nodes have a unique ID.
- Use of non tamper resistant hardware in sensor node.
- If a node is compromised all the key material can be taken out by the adversary.
- The sensor node should be a part of at least one cluster.

4. Proposed work

The proposed framework makes use of keys generated by the base station and the sensor nodes in the cluster to provide the security for both inter and intra cluster communication. This section describes our work in detail. The details of notations are described in table 1

4.1 Framework for enhanced secure key management for hierarchical wireless sensor network

The framework uses the three keys for providing the security in the network. Out of these three keys two are computed by the base station and the third key is computed by the senor nodes in the network by using the localized key material provided to them by the their respective cluster head. One key is used to provide the security between the cluster head and the base station another key is used to provide the inter cluster security i.e. between cluster head and sensor nodes and the third key is used for the securing path between the two neighbor nodes. The path key is generated by the nodes using the nounces supplied to them by the cluster head. Nounce are send on the basis of the distance of the sensor node from their respective cluster head which keeps on changing with the increase in the distance. So the nodes at the same distance will have same nounces and the one which is far off will have lesser nounces. The framework consists of four phases which are Pre Key distribution, Pair wise key establishment, Computing Path key, Re- keying all the keys is discussed below.

4.1.1 Pre key distribution

The WSN is a resource constrained network so to provide a efficient key management the keys should be pre loaded in the nodes before they are being deployed[11].The proposed work to authenticate each sensor node the BS computes a unique key K_{net} and pre loads this key into every sensor node before deployment. This key is deleted after the first round and is used in the cluster formation phase.

4.1.2 Pair wise key establishment

4.1.2.1 Pair wise key establishment between the cluster head and base station

After the nodes are being deployed and pre distributed with K_{net} the BS needs to establish a pair wise key with every cluster head to secure the communication between them so to achieve this BS makes an array V consisting of the id's of all the sensor nodes. After this a cluster head is elected. A node can volunteer himself for being the cluster head else randomly any node is selected as cluster head. After the first round the cluster head can be elected using various scheme like[9,10]After becoming the cluster head for the first time the node sends the authentication message encrypted with K_{net} to

base station which includes its id .The contents of message includes the following

$idCH, idBS$	$EK_{net}(M\|N)$	$mac\ K_{net}(M\|N)$

$M = |idCH\ idBS|K_{net}$
Where M is the message from the CH and N is the timestamp and Mac is generated using the key K_{net} .
After obtaining the message from the CH, BS computes the new key which would be used to for communication between the CH and BS. The new key is generated by applying the one way hash function on the ids of BS and CH i.e.

$$K_{BS-CH} = HK_{net}(V[idCH] + V[idBS])$$

This new key is sent to CH by encrypting the message with the K_{net} .The message from the BS to CH will have

$idCH$	$idBS$	$E\ K_{net}$ $(M\|N\|K_{BS-CH})$	$mac\ K_{BS-CH}$ $(M\|N)$

After receiving the message the cluster head can decrypt he message and obtains the keyK_{BS-CH}.

4.1.2.2 Pair wise key establishment between cluster head and sensor nodes

After becoming the cluster head for the first time the node broadcasts a beacon message to all the nodes in the cluster. The range of beacon message is restricted by using a variable TTL (Time to live) which is initially set to a predefined value and then it gradually decreased with the every forwarding and stops when it becomes zero. The TTL helps in segregating the cluster into different belts based on the distance of sensor nodes from their respective cluster head. Initially the TTL is set to small number like say TTL=3.The beacon message consists of CH id, TTL and Time stamp (to avoid replay attack) all encrypted by the keyK_{net} .

$idCH$	TTL	Timestamp

The nodes in the network can receive several beacon messages from the different cluster heads but can join only one cluster. The CH can broadcast the beacon messages to the SN which are in the transmission range of CH figure 2.

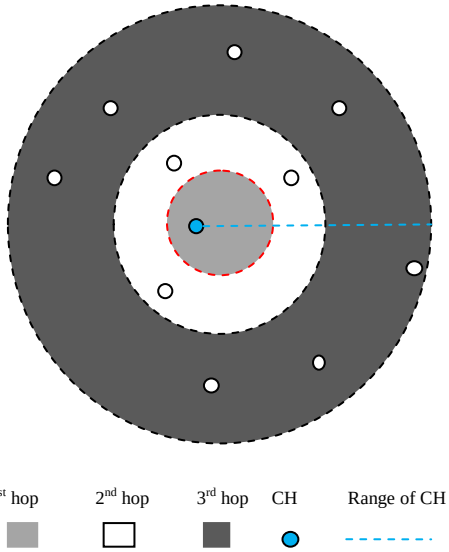

Figure 2: The different hope ranges of nodes from the CH

After receiving the beacon message the node sends a ACK message to cluster head which includes its ID,CH ID, value of TTL when it received by the sensor node and MAC of the message from the cluster head computed using the key K_{net} .

$idCH, idSN$	TTL(Value of TTL When SN received it)	MAC of message from CH

After receiving the ACK message from all the member nodes in the cluster, the cluster head calculates the hop count as

Hop count =TTL_{CH}-TTL_{SN}

for every member node in the cluster. At this point the cluster head has the ids of the every senor node in the cluster. The cluster head sends these id's to BS encrypted by the encrypting it with the key K_{BS-CH} to obtain the cluster key.After receiving the id's of SN's the BS computes the cluster key K_{CH-SN} by using the one way hash function and the pair wise key K_{BS-CH} and then sends the key along with the nounces to the cluster head by encrypting it with the key K_{BS-CH}

$idCH,$ $idBS$	EK_{BS-CH} $(M\|N\|K_{CH-SN})$	$mac\ K_{BS-CH}$ $(M\|N)$	Nounces

After receiving the message from the BS,CH forwards the cluster key K_{CH-SN} and nounces as per the hop count to every sensor nodes in the cluster by encrypting it with the K_{net} . All the nodes decrypts the message to obtain the cluster key and the deletes the key K_{net} .At this point all the nodes in the cluster have cluster key and the nounces according to their distance from the cluster head i.e. node have TTL=3 will have nounces(n1,n2,n3,n4) and node having TTL=2 will have nounces(n1,n2,n3) and TTL=1 will have nounces(n1,n2) figure3

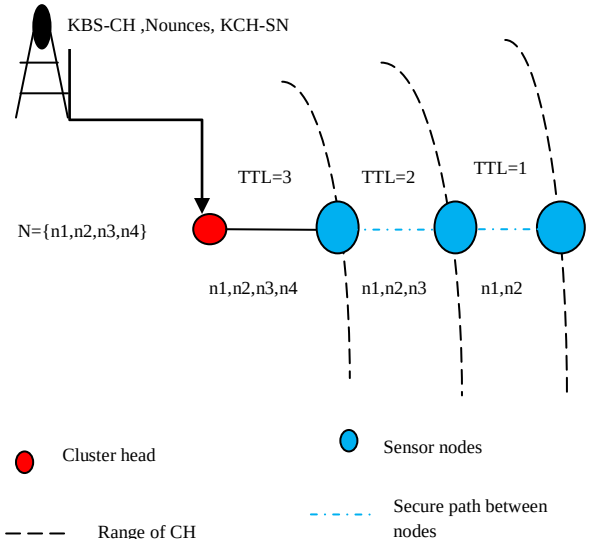

Figure 3: The network setup for TTL=3

4.1.3 Computing the path key

The sensor nodes that are in the same distance range from cluster head receive the same beacon message, so there are matching keys with the nodes. The structure can be viewed from the figure3.These keys can be used to generate the path keys among the sensor nodes in cluster to provide a secure communication between the nodes within the cluster. As per the principal of key generation the two nodes MNi and MNj the set of common keys can be obtained as

$S = LMN_j \cap LMN_i = LMN_j$ as (i< j)

Each MN generates a list which stores the keys as follows

$LMN_j = \{K^i_{MNj} | K^{hops}_{MNj} \ldots\ldots, K^{TTLmnj}_{MNj}\}$

Since all the messages are sent to cluster head and thereafter to the base station so both the cluster head and base station should be able to decrypt the message and get assured for the message authenticity so CH knows the function to calculate the path key which can be shown by the following

$KMN_{ij} = f^{abs\,(i-j)}(K_{CH-SN}, Ni)$

Algorithm for key generation among the sensor nodes to establish a path key

- CH broadcasts the beacon message with different nounces received from the BS
  $CH \rightarrow \{idCH, N, TTL, K_{CH-SN}\}\, K_{net}$
- SN decrypts the $\{idCH, N, TTL, K_{CH-SN}\}\, K_{net}$
- SN deletes the K_{net}
- Key pool for the SN=Null
- $K_{lengt\,h} = TTL_{SN}$
- For i=1 to TTL_{SN}
- {
  $k^i_j = f\,(K_{CH-SN}, \text{ni})$ //generation of key pool using one way hash function on the nounce with the key K_{CH-SN}
  $K^i = K^i \cup \{k^i_j\}$
  }
- End

Sensor nodes use the key K_{CH-SN} to communicate with the CH thus provide enhanced security as communication between the sensor nodes and communication between the CH and SN are both secure. The path key provides the security for communication between the two nodes in the network and the cluster key provide the security for the entire cluster.

Since to provide the authenticity to the nodes in communication CH can verify the keys of the sensor nodes by applying the one way function and get the id's of the nodes. The CH can decrypt the message received from the sensor node by using the following procedure

- Sensor node sends the information to CH encrypted by the key K_{CH-SN}
  $SN \rightarrow \{idSN, idCH, M\}\, K_{CH-SN}$
- CH can obtain the hop count as
  $N_{hops} = TTL_{CH} - TTL_{SN}$
- According to the N_{hops} ,nounce and the one way function the CH can get the idSN and key information
- End

4.1.4 Re-key process

As WSN has limited battery life so to enhance the life of the cluster the cluster head must be changed and to maintain the security all the keys must be re-keyed as it is known that after receiving the certain amount of encrypted messages the use of same key is no longer safe i.e. after receiving more than $2^{2k/3}$ where k is the length of the key[13].So the re-key process starts from the re election of the cluster head.In this way the process of re key starts from the scratch as the new cluster head will require new keys to communicate with the base station and the sensor nodes and more over the distance of all the nodes from the new cluster head will be different from the previous cluster head. So with the new CH the hop count from the cluster head to sensor nodes, nounces and the key material will change.fig4.

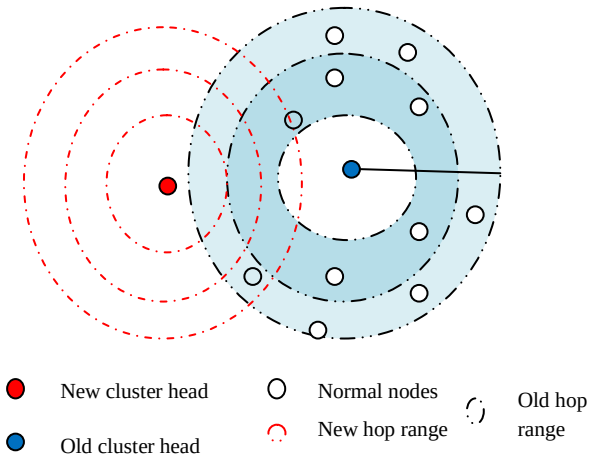

Figure 4: Re-election of cluster head

5. Security Analysis and Simulation Result

This section presents the analysis of the proposed framework and also presents the simulation results.

5.1 Security Analysis

As compared to the all the previous work [4,5,6,8] done in enhancing the secure key management the advantage of our proposed work is that it provides the enhanced security services for both the inter and intra cluster communication in a hierarchical wireless sensor network and also address the challenging runtime security by using the localization of key material and design of robust key generation mechanism. All the previous work done has failed to address the intra cluster communication at the runtime due to this various loop holes in security can be utilized by the adversary to attack the network. Moreover our proposed work doesn't requires any special kind of nodes like RKPH[4],LDK[14] which makes it easy to deploy in practical scenario and also doesn't requires GPS devices. The use of hierarchical network for localizing the key material to nodes and easy hop count mechanism adds advantage to our scheme as compared from other proposed work.

The inter cluster communication is secured by using the path keys which are generated by the nounces and distance. According to the different distance, cluster is further divided into several small security belts and nodes in different security belts have different set of keys to communicate. Since the keys are computed by the set of nounces supplied by the base station the neighboring nodes have some common keys which make them to communicate with other by discovering common keys. As the keys are generated on the basis of hop count the node near to cluster head will have more keys then the other nodes that are far away from the cluster head which makes the far nodes only to submit the message. Moreover all the communication within the cluster is secured by the cluster key which is computed by the base station which makes only legitimate nodes to be a part of communication. This type of security model for inter cluster communication prevents various attacks like eavesdrop, selective-forwarding and hello flood attacks.

The communication is secured from the initial phase i.e. before sending any message it is encrypted using the hash function. Our work also provides the freshness to key management by using the timestamp and nounces. It is always a worrisome to get the key material reveled to adversary after the node has been compromised but our scheme provides a dynamic solution to it as we except that attacker will take some fixed amount of time to compromise the node since the keys are re keyed after some time so by the time attacker will compromise the node the keys would have been changed. The intra cluster communication is secured by using the shared key between the cluster head and the base station which makes the base station to verify the authenticity of the cluster head and this shared key is re keyed every time when a new cluster head is elected for the cluster. By using the proposed scheme for the intra cluster communication the attacks like Sybil attack, acknowledgement spoofing can be prevented. It can also prevents the black hole attack to a large extent and makes sure that the entire network doesn't falls into the hands of attacker.

5.2 Simulation Results

In this section, we evaluate the performance of the proposed framework implemented in MATLAB. The network scenario that we considered consists of 100 nodes randomly distributed we created the network and applied the LEACH [9] for cluster head election. The figure shows the simulation results for the proposed framework. The curve shows the performance of the network communication in terms of the packets sent when there is no security against the security of proposed framework.

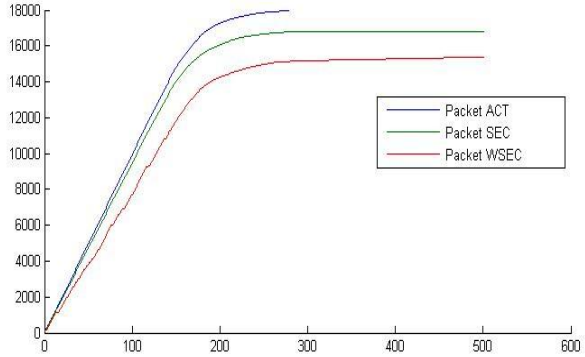

Figure 5: Performance of the proposed framework

The blue curve in the figure shows the actual or the expected packets that can be sent successfully during the life period of the network. The red curve shows the actual packets sent during the lifetime of the network and under the presence of the malicious nodes. The green curve shows the packets sent with the security of the proposed framework during the entire life time of the network.

6. Conclusion and Future Work

In this paper we propose the new framework for enhancing the security of a hierarchal wireless sensor network against the various attacks .In contrast to other proposed schemes our work addresses the challenging runtime security issues and also provides the robust mechanism for continuous authentication of nodes in the network. Our work divides the cluster into smaller isolated geographical belts on the basis of the distance from the cluster head which provides the tight security inside the cluster. The uses of separate unique keys for both inter and intra cluster communication makes our work more resilient against the various attacks that can be carried out on the network. All the keys used for communication are rekeyed after the fixed time which makes it difficult for the adversary to know the keys from the network. In the future we will focus on how to enhance the security in mobile and scalable WSN's.

Table.1

Notations	Description
idSN	Identification number of sensor node in network.
idCH	Identification number of cluster head.
idBS	Identification number of base station.
K_{net}	Network key stored in each sensor node before deployment.
K_{BS-CH}	Pair-wise key shared between the base station and cluster heads.
N_{hops}	Number of hops
EK(M)	Encryption of the message M with key K.
V	Array of the node id's.
Mac M(K)	Message authentication code for message M using key K.
MNi	Member node i in the cluster.
Ni	ithnounce in the set of nounce N.
$f()$	One –way function
k_j^i	ith key for the member node MNj.
K_{CH-SN}	Pair-wise key shared between the cluster heads and the sensor nodes

7. REFERENCES

[1] L. Eschenauer, V_D. Gligor, A key management scheme for distributed sensor networks. In: Proceedings of the Ninth ACM conference on Computer and communication secuirty (CCS '02.), pp.41-47,2002.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the IEEE Symposium on Security And Privacy, pp. 197–213, 2003

[3] S Zhu, S Setiaand S Jajodia "LEAP: efficient security mechanisms for large-scale distributed sensor networks" in the proceeding of 10th ACM conference on Computer and communication security(CCS'03),pp.62-72,2003.

[4] S. Banihashemian and A. G. Bafghi, "A new key management scheme in heterogeneous wireless sensor networks," in Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT '10), pp. 141–146, February 2010.

[5] Y.Y. Zhang, X.Z. Li, J.P. Cao, L.K. Zeng, Y. Zhen and D.Q Gao "Distance-Based Key Management in Hierarchical Wireless Sensor Network" in the proceeding of Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on Digital Object Identifier, pp. 915 – 918,2012

[6] Yiying Zhang,,Xiangzhen Li, Jianming Liu, Jucheng Yang, and Baojiang Cui "A Secure Hierarchical KeyManagement Scheme in Wireless Sensor Network" International Journal of Distributed Sensor Networks,Volume 2012 ,pp 1-8, 2012.

[7] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 24–34, 2007.

[8] AbdoulayeDiop, Yue Qi, Qin Wang, and ShariqHussain "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks" International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012,pp 365-370,2012.

[9] Heinzelman,WendiRabiner,AnanthaChandrakasan and HariBalakrishnan"Energy-efficient communication protocol for wireless sensor networks" In System Sciences,2000.Proceedings of the 33rd Annual Hawaii International Conference on IEEE,pp 10-pp,2000.

[10] Manjeshwar and D. P. Agrawal, "TEEN: a protocol for enhanced efficiency in wireless sensor networks," in Proceedings of the 15th international workshop on parallel and distributed computing issues in wireless networks and mobile computing, pp. 2009–2015, 2001.

[11] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks, vol. 2, no. 4, pp. 500–528, 2006.

[12] Martins,David and HerveGuyennet"Wireless sensor network attacks and security mechanism:a short survey".IN the Proceedings of 13th International Conference on Network –Based Information System(NBiS),pp.313-320.IEEEE,2010 [For security analysis].

[13] H. N. Seyed, H. J. Amir, and D. Vanesa, "A distributed group rekeying scheme for wireless sensor networks," in ProceedingsofThe 6th International Conference on Systems and NetworksCommunications (ICSNC '11), pp. 127–135, 2011.

[14] Anjum and Farooq" Location dependenet key management in sensor network without using deployment knowledge" in Wireless Networks 16,no.6(2010),pp.1587-1600,2010.