Scientific Research and Essays Vol. 7(47), pp. 4060 -4070, 3 December, 2012
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE12.371
ISSN 1992-2248 ©2012 Academic Journals

Full Length Research Paper

Enhanced efficient group key transfer scheme for wireless sensor networks

[1]Annlin Jeba S. V.* and Paramasivan B[2]

[1]Department of Computer Science and Engineering, C.S.I Institute of Technology, Thovalai, Tamil Nadu, India.
[2]Department of Computer Science and Engineering, National Engineering College, Kovilpatti, Tamil Nadu, India.

Accepted 17 October, 2012

Wireless sensor networks (WSNs) have become a motivating technology as it can be constructed without communication infrastructures. WSN operates in harsh environment; therefore information security in infrastructureless WSN is one of the most important challenges. WSN possess different network architectures. Cluster-based WSN architecture is found to be efficient with reduced transmission power and low energy consumption. To enhance the purpose of cluster based WSN, it is necessary to protect the communication within a cluster. This paper focuses on cluster-based key management scheme. Further in this paper, a mathematical model is used to securely share key among the communicating entities in a group. Moreover, the proposed scheme prevents impersonators from accessing any information exchanged within a group. Security analysis shows that proposed scheme maintain a good level of security. Performance evaluation illustrate that proposed scheme is performed with minimum computation and communication overhead.

Key words: Group key, intra cluster, authentication, interpolation, sensor network.

INTRODUCTION

In sensor network applications, the sensor nodes are deployed in application specific region. Each sensor node senses the environment and collects the information from the field of interest. The sensed information collected from nearby sensor nodes has to be aggregated and then aggregated report has to be forwarded to the BS. In order to perform data aggregation, the network has to be organized into groups or clusters. Each cluster has a coordinator known as CH.CH aggregates the data collected from its cluster and forward them to Base Station. In clustered network, the communications are divided into intra cluster and inter cluster communication. To make use of the advantages of clustered network communication (Wei et al., 2008), it is necessary to protect communication within a cluster. Security services such as confidentiality and authentication has to be considered for the design of secure group communication. Confidentiality is achieved through key management. Group key is used for securing the group communication (Li et al., 2008) and prevent the adversaries from retrieving the information communicated within the group.

Authentication is carried out through MAC (message authentication code) endorsed along with event information. Key management includes key generation, key distribution or sharing, storage and authentication between nodes. There are number of traditional key distribution schemes, most of which are not suitable for WSN. For example, public key based distribution cannot be used for WSN because of its high processing requirements; global keying scheme is not applicable because of its security vulnerabilities. Centralized key distribution scheme need a trusted third party to produce session key. The drawback of this scheme is that, it is susceptible to single point failure. In key pre-distribution schemes, the sensor nodes store many useless keys and waste the storage space of the sensor nodes. Group key establishment protocols (Chadha et al., 2005) are categorized into key agreement and key transfer protocols. In key agreement protocols (Amir et al., 2004),

*Corresponding author. E-mail: annlin_jeba@yahoo.co.in.

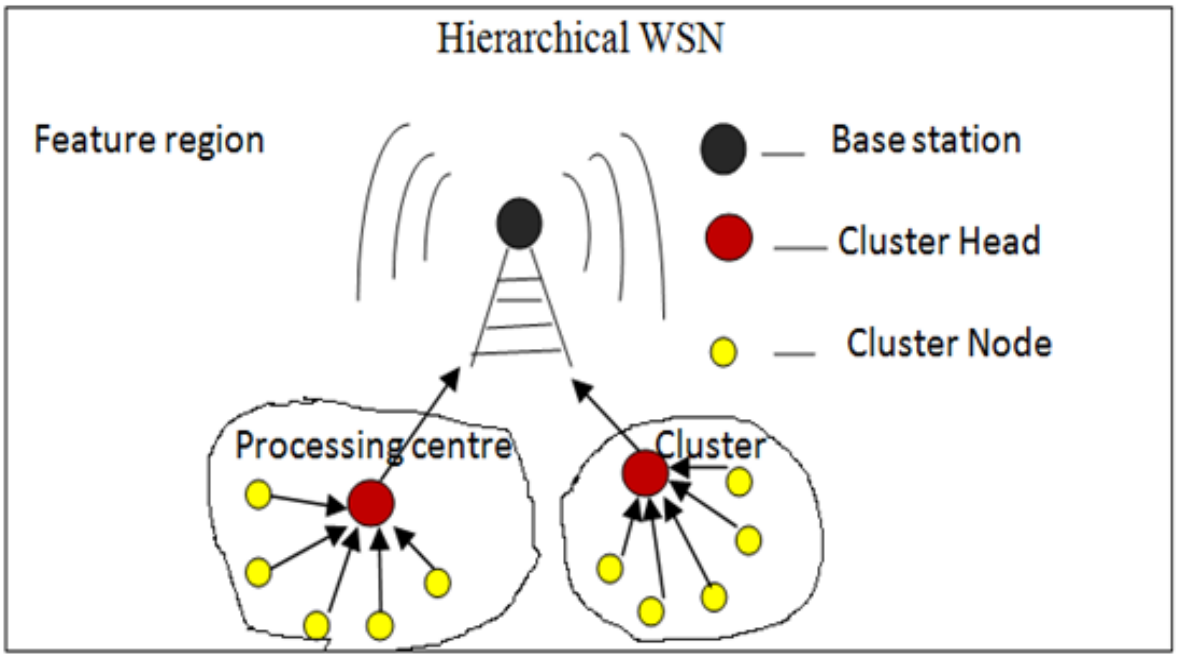

Figure 1. Hierarchical cluster-based WSN.

all sensor nodes in the cluster are involved to generate group keys. The time delay of setting up this group key may be too long when there are large members in the cluster. Key transfer protocols depend on a trusted entity in the cluster, CH.CH generate and transfer group keys secretly to all members in the cluster. Secure group communication requires scalable and efficient group membership management. Group membership management includes suitable access control measures to prevent unauthorized access and eject compromised node. Moreover, when a sensor node joins a cluster, it must not be able to access the group communication earlier to its joining. When a sensor node leaves a cluster, it must be prevented from accessing any further group communication.

The purpose of this paper is to generate and securely share key within a group for inter and intra cluster communication. In the proposed scheme, each cluster contains minimum number of cluster members which enhances the cluster management process. Moreover, the proposed scheme adopts an efficient authenticated key sharing mechanism. This mechanism requires only two messages exchanged between communicating entities for rekeying. Existing schemes follow cryptographic techniques for key sharing. But the proposed scheme uses a mathematical model for key sharing, which is theoretically and practically more accurate. When a new communication is to be established, rekeying (Wang et al., 2007) will be performed to enhance key refreshness in the group. This scheme not only ensures the security of data communicated in the cluster, but also lowers the complexity of the communication procedures.

PROBLEM STATEMENT

System model

The proposed scheme considers a hierarchical cluster-based WSN. The sensor nodes which are in close proximity are grouped into clusters. Each cluster is controlled by a cluster head which co-ordinates information from all other sensor nodes in its cluster. CH sends aggregated report to the base station which is considered as trust worth. The clusters may be organized based on the region where they are present. The network architecture is depicted in Figure 1. The hierarchical organization of WSN ensures the reduction in number of messages broadcasted from BS to individual nodes. It also reduces the management overhead on the BS.

Threat model

In the proposed scheme, cluster head is assumed to be a trusted node. This scheme considers an attacker that tries to capture and compromise sensor nodes in a group or cluster. When a node gets compromised, adversary can acquire all the information maintained in that node. Also, it is assumed that adversary does not have prior

knowledge of what is stored at each node and cannot selectively direct the attack towards a particular node. Furthermore, adversary is able to compromise the nodes involved on routing. The proposed scheme prevents unauthorized access of adversaries from inside as well as outside the WSN through group key management. Moreover, this scheme is able to detect and eject the compromised nodes along the path of data transfer through authentication among associated nodes in the path.

Problem definition and design goal

The objective of this paper is to develop cluster-based authenticated group key. The sensor nodes in the application specific region are partitioned into groups or clusters. After organizing the nodes into clusters, the communication path between source cluster and BS has to be identified and authenticated. The key sharing mechanism used here is considered efficient since this scheme require a mathematical model to compute and share group key. Moreover, this scheme requires only few messages to be exchanged between communicating entities for authentication and secure key generation. Hence, require O(2) messages for rekeying. When a sensor node leave or join a cluster, rekeying will be performed to enhance security.

Design goal

i) Scalable, manageable region based clustering scheme.
ii) Mathematical model for group key generation and sharing.
iii) Each and every node along the path to BS is authenticated using hash based authentication mechanism.
iv) Enhanced forward and backward security.

RELATED WORKS

Cluster based WSN architecture is one of the leading scheme for energy efficient communication. Clustering minimizes the transmission power and balance the load among the nodes for prolonging the network lifetime. Cluster based secure communication in WSN is a challenging issue that has been addressed throughout several research works.

Clustering schemes

The main goal of cluster based WSN architecture is to maintain energy consumption of sensor node. The energy consumption can be minimized by multi-hop communication within a cluster, and by aggregating the data transmitted to BS in order to reduce the number of messages transmitted to BS.

LEACH [(Heinzelman and Chandrakasan, 2002) Low Energy Adaptive Clustering Hierarchy] is the first clustering algorithm that was proposed for reducing power consumption in WSNs. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS). But LEACH is not applicable to networks deployed in large regions.

HEED [(Younis and Fahmy 2004) Hybrid, Energy-Efficient Distributed] Clustering is another distributed clustering approach. In this approach, the cluster heads are selected periodically on the basis of two parameters, the residual energy and cost incurred during the intra clustering communication. The HEED clustering improves network lifetime over LEACH clustering because LEACH randomly selects CHs (and hence cluster size), which may result in faster death of some nodes.

TEEN [(Manjeshwar and Grawal 2001), Threshold Sensitive Energy Efficient Protocols] TEEN is suitable for time-critical sensing applications. Moreover, this protocol is quite efficient in terms of energy consumption and response time. The main disadvantage of this scheme is that when periodic reports are needed, and if the threshold is not received, the user will not get any data from the network at all. This scheme inappropriate for periodic monitoring of events.

APTEEN [(Manjeshwar and Agrawal 2002) Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol]: APTEEN is an improvement to TEEN to overcome its limitation and aims at both capturing periodic data collections as LEACH and reacting to time-critical events as TEEN. Compared to LEACH, TEEN, APTEEN consumes less energy. Drawbacks of TEEN and APTEEN are Overhead and complexity of forming clusters in multiple levels and implementing threshold-based functions. The clustering scheme presented in this paper is able to overcome the drawbacks of the existing schemes. The proposed scheme does not require any specific parameters or threshold specific values for clustering. Moreover the proposed scheme is scalable and manageable with increased life time compared to other related schemes.

Key management in WSN

Group key is one of the most important key management paradigms, for secure group communication which is both bandwidth-efficient and energy-efficient. Group key management protocols (Chadha et al., 2005) can be of two types; centralized group key management and distributed group key management protocol. In centralized group key management, a trusted authority is required to generate and share keys to other

communicating entities in the group or cluster. In distributed group key management, each member of the group contributes to the key generation and distribution. In distributed key management schemes, the key agreement protocols are involved in key generation and distribution. In the proposed scheme, key generation and sharing is performed by a trusted authority. There has been some work on secret sharing using some trusted authority.

Zhang and Cao (2005) proposed a group rekeying scheme for filtering false data in sensor networks. In their scheme, the group is defined as the immediate neighbouring nodes around a sensor. The BS initiates group key updating at each session. Each node obtains the new group key through collaboration with certain number of neighbours. This scheme is high in security but there are computational, storage and communication overhead. One group based re-keying scheme proposed by Asem et al. (2006) is a computationally efficient key hiding based group re-keying scheme in which keys are hidden in a numerical matrix and is sent to the group members. Each group members extract the key from the matrix by using secret stored by each group member initially. This keying mechanism cannot be applied to WSN containing thousands of nodes scattered in a sensor field because large sized networks require large size matrix resulting in large size message. But this scheme can be applied for cluster based WSN where CH takes the responsibility of re-keying.

Eltoweissy et al. (2004) proposed an Exclusion Basis System (EBS) for efficient group key management and to reduce the number of messages for re-keying in group communication. Re-keying messages are in a way that only legitimate nodes can decrypt the message. In EBS, each node has k keys out of pool containing C (k + m, k) keys. If a node is found to be compromised, to evict the compromised node ‘m’, new keys were distributed which are not known to the evicted node. Communication overhead increases with the increase in value of ‘m’. Storage requirement increases with increase in value of ‘k’. EBS is scalable for large scale networks. One drawback of EBS scheme is vulnerable to collusion attack. In EBS, only few messages are sent for replacing the old keys. Younis et al. (2006) proposed a scheme which was called Scalable, Hierarchical, Efficient, Location-aware and Lightweight. SHELL performs location-based key assignment in a cluster to decrease the number of keys revealed by a collusion of attackers. Nearby sensors in SHELL, share more common administrative keys than distant sensors and each cluster heads need to have more size of memory compared to other schemes.

In SHELL, key renewal occurs within each cluster. In SHELL, collision is reduced by using node’s physical locations in computing their keys. Moreover, the nodes need to collude to reveal the information about the network is more in number; hence, it is difficult to perform node capture attack. Here, the responsibility for rekeying is distributed among CH, cluster gateways. Here results in high communication overhead.

Du et al. (2006) proposed localised combinatorial keying (LOCK) which employs EBS scheme developed by Eltoweissy et al., in 2004 for key renewal between CH and its member in a group. LOCK does not use location information in generation of keys. In LOCK, if an adversary compromises any node, it does not have an effect on the operations of node in other clusters. Further LOCK used key polynomials to improve network resilience to collision instead of location based key assignment in SHELL. Chia-Yin et al. (2011) proposed an efficient authenticated group key transfer protocol with the knowledge of any ‘t’ or more than ‘t’ shares’; it can reconstruct the secrets easily. With knowledge of fewer than t shares, it cannot recover the secret S. This scheme uses a mathematical method to share secret between CH and its members. Moreover, Harn and Lin (2010) scheme require an online key generation center to construct and transfer the group key which increases the overhead required to implement the system. Further KDC is susceptible to single point failure. This scheme cannot be used for real life application.

Leonardo et al. (2007) intend to secure LEACH by using a probabilistic scheme. In SecLEACH, each node has ‘k’ predetermined keys obtained randomly from a set of keys ‘p’. The main advantage provided by SecLEACH is the possibility to authenticate and to secure the communication between CH and cluster’s members without the partition. Overhead in SecLEACH is due to the factors such as message size and increased node CH distance. Gianluca and Maria (2011) proposed a lightweight authenticated rekeying scheme, LARK. LARK achieves security and scalability by using two mechanism key chain, key graph. LARK requires a distributed application-specific architecture with more than one BS. Moreover, LARK guarantees forward and backward security to prevent any new cluster member access the key prior joining or using the current group key. But in LARK’ grouping is not easy and also result in communication overhead. Also, there is only one key server, no CHs so each sensor node store keys.

PROPOSED SCHEME

This paper proposes a reliable cluster based group key management scheme for secure and authenticated group key transfer. Here, the trusted entities, CH and BS perform scalable and efficient group membership management with appropriate access control measures. Every time a membership change occurs, the group key must be refreshed to ensure backward and forward secrecy. Backward secrecy means that a node joining the group must not reveal previous exchanged information. Forward secrecy means that a node leaving the group must not reveal future exchanged information. Moreover, the proposed secret sharing scheme must resist internal node compromisation, since any information shared among group members is secure and cannot be

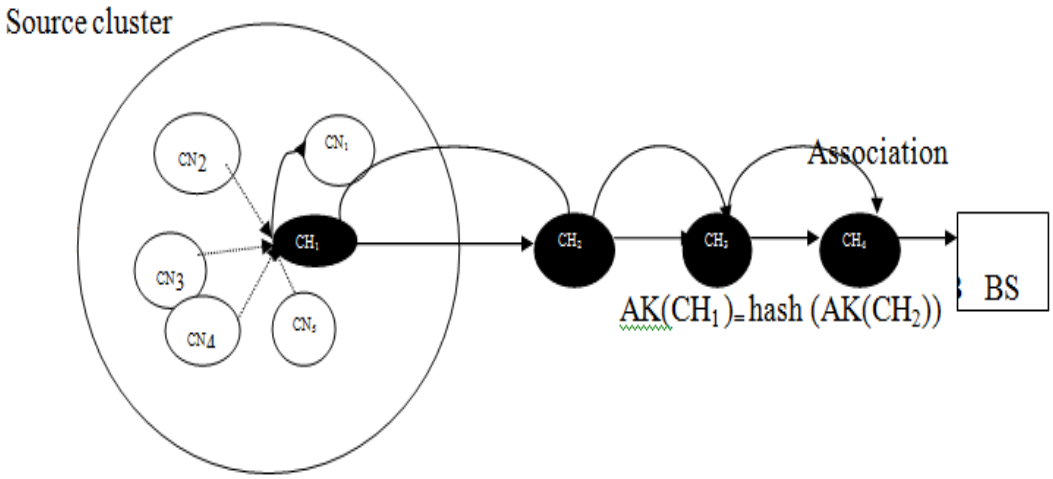

Figure 2. Associated key for authentication.

disclosed. When secured data is transferred from source cluster head to BS, the en-route nodes along the path of data transfer has to be authenticated to avoid internal node compromisation.

Scheme overview

The proposed scheme is divided into four phases. The important notations used are given in Table 1.

Cluster organization phase: Initially, the sensors are deployed in a field of interest. After deployment, the sensor nodes are partitioned into clusters of equal size. Each cluster is controlled by a CH. One node in the WSN is assigned as the BS, which is trust worthy and contains all the keys for other sensor nodes.

Authentication phase: After organizing the cluster, the path for inter cluster communication has to be identified and authenticated. In the proposed scheme, authentication is performed by means of associated key distributed by the BS. Forward as well as backward authentication is performed by means of association established between consecutive nodes along the path. Moreover, cluster members are authenticated by the CH using the associated key shared by the CH with its members. In the association discovery phase, a node discovers the ids of its associated nodes. This process may be initiated by the BS periodically.

Group key generation and distribution: Group key is generated by the CH or BS and shared between the CNs and CHs by Newton's divided difference interpolation method. The group member or cluster nodes should register with the CH. CH share secrets with each cluster members. Group key can be shared among the group members by generating a polynomial expression using the secret share received from the CH.

Detailed procedure

Cluster organization phase

After deployment of the sensor nodes in the area of interest, the sensor nodes are organized into clusters. Clustering is the process of partitioning a given set of sensor nodes into k groups or clusters based on some metrics. Clustering is required to reduce the routing overhead and for effective energy efficient communication between nodes. In the proposed scheme k-means clustering algorithm is followed for grouping the nodes into clusters. This algorithm is used in the proposed scheme for clustering because this algorithm does not require any specific metrics to organize the sensor nodes into clusters and is computationally faster than other clustering methods. The k-means clustering algorithm performs the following steps for clustering. Let $S = \{s_1, s_2, s_3 \ldots s_n\}$ be the sensor nodes deployed in Euclidian space R^N

1) Choose a number of desired clusters, k.
2) Choose k sensor nodes randomly among n deployed sensor nodes to function as cluster head $\{CH_1, CH_2 \ldots CH_k\}$ in R^N
3) Assign the remaining nodes to their closest CH. For each CH_i, i € {1…k} set the cluster C_i be the set of five nodes in S that are closer to the cluster CH_i.
4) Construct the cluster in such a way that each cluster should contain maximum of six nodes.
5) Repeat step 3 in such a way for each cluster C_i set the CH_i to be the center for all the points in cluster C_i. The same procedure has to be repeated until there is no change in CH_i.
6) The distance between CH_i and other sensor node within a cluster is given by $||CH_i - S_j||$

Thus WSN is organized into hierarchical clusters based on the region where CH and group of nearby sensors are present. The clusters are arranged in a hierarchy with the root as the BS and all other CHs are linked with the BS.

Authentication phase

Once the network is organized into clusters, CH identifies their members by sending some control message. Before initiating the communication with BS, every source CH should identify and authenticate the communication path. In the proposed scheme, BS determines the shortest path as the suitable path for communication with CH. For authenticating the nodes along the path of data transfer, BS distributes associated key (AK) to CHs closer to the BS on the selected path. Figure 2 shows associated key generation scheme; the association discovery phase is necessary for a node to discover the AK of its associated nodes. Moreover, node closer to the BS is called upper associated node. All other associated nodes including source CH generate AK from

Table 1. Notations in proposed mechanism.

Symbol	Definition
CN_{id}	Cluster Node's identity
CH_{id}	Cluster Head's identity
AK	Associated Key
R_i	Random Nonce
CN_{AK}	Cluster Node's Associated key
CH_{AK}	Cluster head's Associated key
BS_K	Base Station key
||	Concatenation operator
H( )	One way hash function
(X_i,Y_i)	Secret share of each node, x-coordinate, y-coordinate

the result of hash function of upper associated node's AK. Source CH distributes AK to all other cluster members. By this way, key storage overhead and key information loss by compromising node on the path can be reduced. The CH acknowledgement process can be omitted by letting a lower associated node include its id with its MAC when it forwards a report.

Secret sharing phase

Secret sharing has been used to distribute or share a key among the communicating entities in a group or cluster. Before exchanging communication messages in a group, a group key establishment protocol need to distribute one-time secret session keys between the trusted entity and other members in the group. The proposed scheme uses secret sharing technique to replace the existing encryption algorithms which was used to enhance confidentiality of group key. In this scheme, each cluster member should register at a trusted entity, CH. The CH share a secret with each cluster member. Also, CH broadcast secret shares to all cluster members. Moreover, proposed scheme uses Newton's divided difference interpolation polynomial scheme for computing secret key by the communicating entities. Newton's divided difference interpolation is computationally efficient to add more sensor nodes for deriving higher order interpolating polynomial. But other interpolation schemes are inefficient against scalability with more mathematical operations and memory for storage. Moreover, the mathematical model illustrates special case of information theoretic privacy. Here, mathematical model is used for key sharing, since no information about the message is exposed without the knowledge of the key. In the proposed scheme, secret sharing can be performed in two different ways:

1) Intra cluster secret sharing (sharing between CH and other ordinary nodes in the cluster).
2) Inter cluster secret sharing (sharing between CH and the BS).

Intra cluster secret sharing

When a sensor node in a cluster wants to communicate to the CH, it needs an authenticated group key to be shared between the communicating entities in the cluster. The proposed group key sharing scheme contains the following steps:

i) Initiating source cluster node sends a group key generation request along with the list of its group members $\{CN_1, CN_2 \ldots CN_5\}$ to the CH.

ii) The CH after receiving the request from the initiating cluster node, broadcast the list of all participating cluster members $\{CN_1, CN_2 \ldots CN_5\}$
iii) Each cluster member need to send a random challenge R_i (i = 1, 2...5) to get registered to their CH. Each CN_i compute an authenticated message which include:

$$H(CN_{id}||CH_{id}||CN_{AK}||)\oplus R_i = TR_i \quad (1)$$

iv) CH receives the message and get the random value R_i through exclusive XOR operation where:

$$TR_i \oplus H(CN_{id}||CH_{id}||CN_{AK}||) = R_i \quad (2)$$

v) CH selects a group key k, generates a polynomial f(x) using Newton's divided difference interpolation passing through (t+1) points (0, k) and $(x_i, y_i \oplus R_i)$ where t refers to the total cluster members in the source cluster, i = 1...t. Also, CH share the secret $(x_i, y_i \oplus R_i)$ with each participating ordinary cluster nodes.
vi) Each ordinary cluster nodes after receiving the secret share able to compute the polynomial f(x) and obtain the group key k = f(0). Figure 3 shows intra cluster group key generation steps.

Given 'n' sensor nodes in a cluster, the Newton divided difference polynomial of degree n-1 can be formed from corresponding n points of the nodes as:

$$P_{n-1}(x) = f[x_0] + \Sigma^{n}_{k=1} f[x_0, x_1, x_2 \ldots x_k] (x-x_0)\ldots(x-x_{k-1}) \quad (3)$$

Where $f[x_0, x_1, x_2 \ldots x_k]$ denote k^{th} divided difference of f with respect to $x_1, x_2 \ldots x_k$

Inter cluster secret sharing

In Inter cluster communication, source CH communicate with BS through trusted CHs along the path. The proposed key sharing scheme contains the following steps:

i) Source CH sends a request for session key generation to the BS along with the list of CHs along the path of communication.
ii) The BS after receiving the request from the initiating CH, broadcast a list of all participating CHs to all CHs involved in the communication.
iii) Each CH sends a random challenge R_i to the BS. CH compute an authenticated message which include:

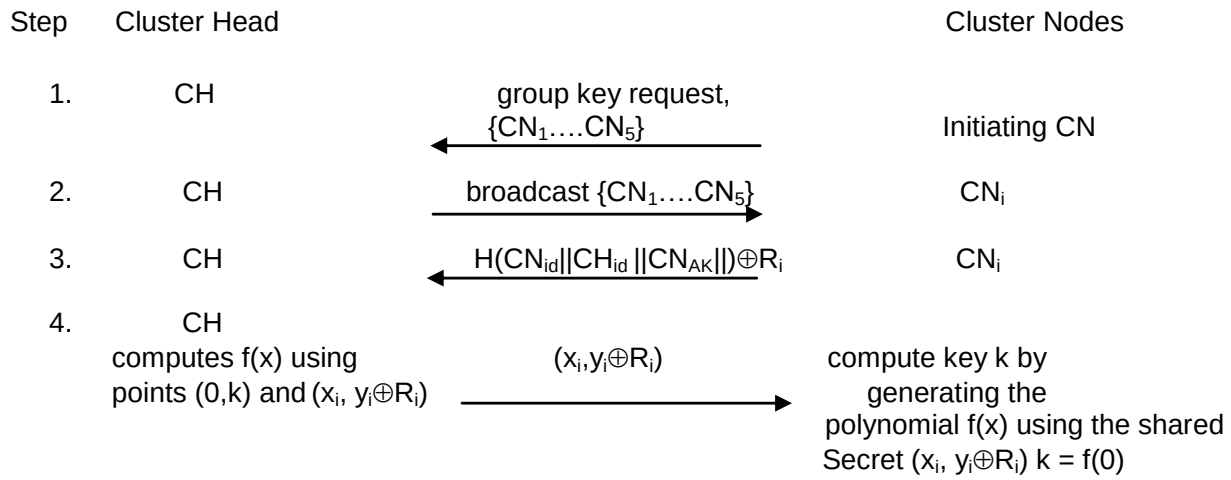

Figure 3. Intra cluster group key transfer.

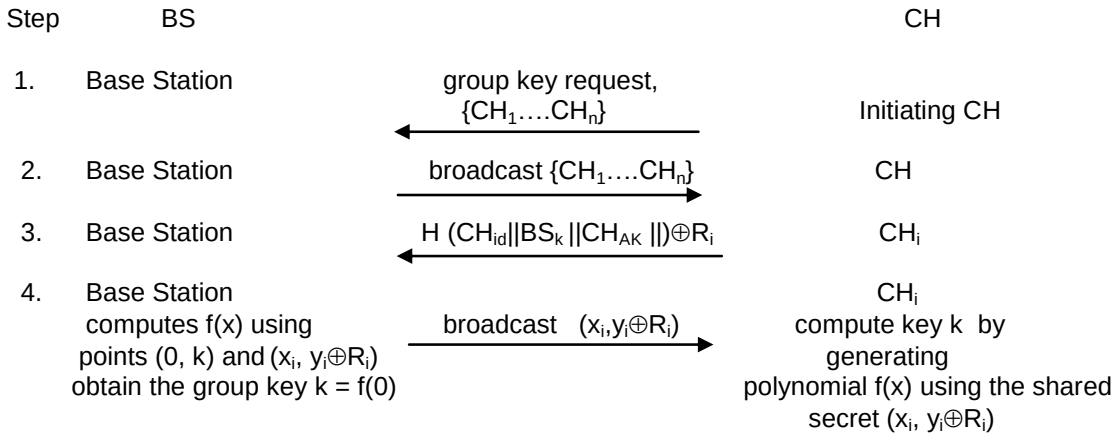

Figure 4. Inter cluster group key transfer.

$$H(CH_k||BS_k||AK_{CH}||)\oplus R_i = TBR_i \quad (4)$$

iv) BS receives the message and get the random value R_i through exclusive XOR operation where:

$$TBR_i\oplus H(CH_k||BS_k||AK_{CH}||) = R_i \quad (5)$$

v) BS selects a group key k, generates a polynomial f(x) using Newton's divided difference interpolation passing through (t+1) points (0, k) and $(x_i, y_i\oplus R_i)$ where t refers to the total CHs involved in the communication and I = 1..t. BS share the secret $(x_i, y_i\oplus R_i)$ with each participating ordinary cluster nodes.
vi) Each CH after receiving the secret share able to compute the polynomial f(x) and obtain the group key k = f(0). Figure 4 shows inter cluster group key generation steps.

Given 'n' CHs in the path to the BS, the Newton divided difference polynomial of degree n-1 can be formed from corresponding n points of the CHs as:

$$P_{n-1}(x) = f[x_0] + \Sigma^n_{k=1} f[x_0, x_1, x_2\ldots x_k](x-x_0)\ldots(x-x_{k-1}) \quad (6)$$

Where $f[x_0, x_1, x_2\ldots x_k]$ denote k^{th} divided difference of f with respect to $x_1, x_2\ldots.x_k$

Key refreshing

Add new nodes: When a new node wants to enter into the network, it needs to inform the BS about its arrival. The BS identify the cluster nearest to the location of the new node and sends information to the CH about the arrival of a node in its region. CH send a control message along with its key to the new node. The new nodes get registers with the CH. Then, CH unicast AK to the new node. The CH initiates rekeying by broadcasting new secret shares to its members to compute the new key to enhance key refreshness and to secure group communication.

Delete nodes: When a sensor node leaves or forced to leave a cluster due to internal node compromisation, leaving sensor node must be prevented from further accessing the communication shared in the group. Hence, when a sensor node leaves the cluster, this should be notified to the CH or if a sensor node gets

Table 2. Comparison of security between proposed and other schemes.

Schemes measurement	SHELL	LARK	Proposed
Clustering scheme	Disjoint clusters	overlapping	Region based
Authentication	No authentication	Key-chain	Associated key
Group Key secrecy	More complex	Weak secrecy	More efficient
Communication message	O(n)	O(log n)	O(2)

compromised this will be monitored by the CH. To enhance key refreshes, the CH initiates rekeying by broadcasting new secret shares to its members except the one that leave the cluster to compute the new group key.

SECURITY ANALYSIS

Here, some comparison and analysis on security level is performed between the existing and proposed schemes. Comparison of security between the proposed and related other schemes is listed in Table 2.

Clustering

Sensor nodes are inexpensive with low power. Hence, energy use is an issue in designing sensor network. To reduce energy consumption cluster based WSN has been proposed. The efficiency of the clustering method used in the proposed scheme can be determined by comparing with clustering methods used in related schemes SHELL, LARK. In SHELL, sensor nodes are partitioned into disjoint clusters. Communication between sensor node and CH within a cluster is through one hop or multihop transmission. Also, in each cluster, sufficient numbers of gateways are deployed to ensure area coverage. Cluster management is spread among multiple nodes (gateways, CH) within a cluster which include complex operation. LARK represents an application specific clustering scheme with multiple BS. Here, a sensor node can be a member of more than one cluster. Further communication overhead occurs due to overlap cluster operations. But in the proposed scheme region, based and application specific clustering is performed. Sensor nodes in a cluster are within the transmission range of CH.

Communication between sensor node and CH within a cluster is through one hop transmission. Proposed scheme is considered to be energy efficient compared to other related schemes.

Authentication

An authentication mechanism is used to verify the information exchanged between communicating entities. SHELL does not use any specific technique for authentication. Each new group key is encrypted by its predecessor key and then broadcasted to group member with the hope that only the right member can get the group key. LARK achieves key authenticity through key chains. In the proposed scheme, associated keys (AKs) are used for authentication purpose. Further, in proposed scheme there is no relation between AK and group key, but in LARK, group key is based on keys used for authentication. Hence, proposed scheme is more secure compared to existing schemes.

Group key secrecy

An adversary may try to break secret key and extract confidential information from the messages exchanged between communicating nodes in the group. Hence, it is necessary to refresh keys at appropriate time intervals. In SHELL group, key will be generated by a CH and send to the gateways within the cluster. Gateways encrypt the group key using administrative key known by each sensor node and send to other CHs. Further CH send the encrypted key to the sensor nodes. The number of communications involved in key transfer is more and this occurs as overhead. Further sensor nodes can easily get compromised since one key will be known by more number of nodes. In LARK, the key server generates chain of authentication key and issue the current key to the group members. Group member receives some authenticated trigger command from key server to compute new group key when a sensor node join or leave the group. Here, group key is generated by applying a mixing function on current keys from key chain and inverted key chain.

In LARK, the forward secrecy can be broken if nodes in close proximity belong to the same cluster. But in the proposed scheme, group key will be computed by individual sensors. Any information exchanged between CH and CNs for group key generation is secured and authenticated.

Order of message

Order of message represents the number of messages communicated between CH and sensor node for rekeying. In SHELL, ‘n’ messages are communicated between CH and the sensor node for group key sharing, where n refers the size of the group. LARK requires ‘n-1’ messages for rekeying purpose. In the proposed scheme only two messages are communicated between CH and the sensor node in a group for rekeying. Keys computed own the property of key independence. If more information is to be communicated in need of group key generation, some information can be disclosed to adversary. Hence, it is necessary to reduce the number of communicated messages.

SIMULATION RESULTS

Simulation is carried out using NS2 simulator with 500 nodes deployed in 1000 × 1000 m. Experiment is performed with groups of different sizes. To compare the efficiency of proposed scheme with prevalent ones, the following metrics are used.

Resilient to node compromise

Resilience against node compromise measures how an adversary can attack a sensor node after the network is deployed.

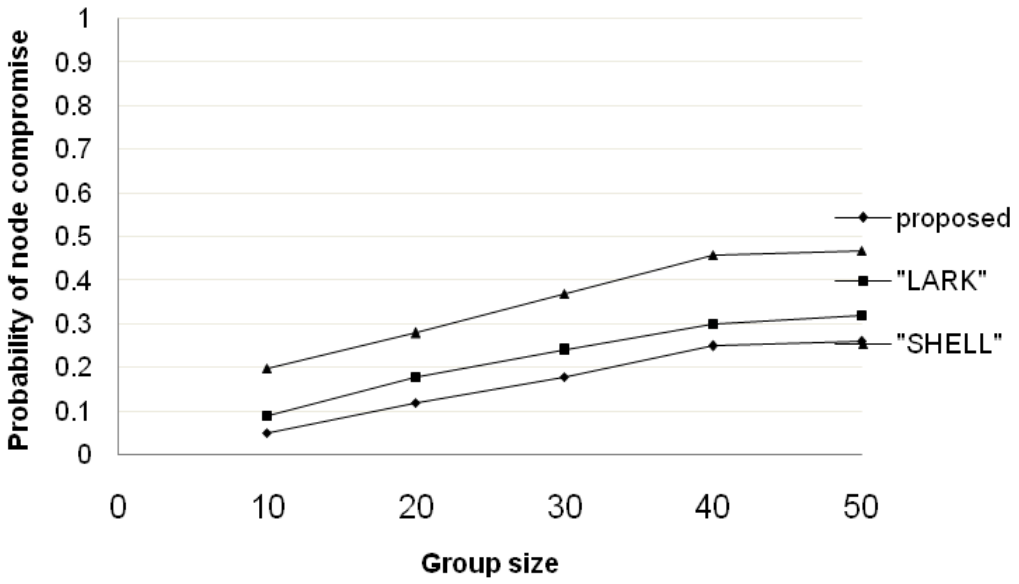

Figure 5. Probability of node compromise.

Computational complexity

Computational complexity measures the computation time required for rekeying.

Key storage space

Key storage space measures the total memory usage for measuring keys in the network.

Resilient to node compromise

In the proposed scheme, node compromisation cannot be a success for an adversary because for each data to be communicated within the cluster, group key will be refreshed. Every information communicated will be secured and authenticated in such a way that unauthorized user was unable to eavesdrop the information on transit. Even though the message is eavesdropped, content cannot be disclosed. Also, in the proposed scheme, the polynomial used for key generation will be refreshed. But in the existing scheme such as SHELL where a node shares more than one key with multiple nodes in proximity; so it is easy to compromise the nearby nodes by exposing common shared keys. Figure 5 shows the node compromise level of different schemes. Moreover, the requests from group members are not authenticated. In SHELL, if the IDS in CH do not function well, SHELL does not guarantee good performance. In LARK, it is assumed when a new node join a cluster it is not compromised. The IDS components present in key server monitor the activities in the cluster to uncover compromised nodes. But how it is performed is not explained. When IDS detect a node as compromised, compromised node will be ejected by refreshing group key. Adversary receives all the keys from the compromised nodes.

In LARK, forward security can be violated if the adversary succeeds in combining keys obtained from compromised nodes. Moreover, in LARK, if nodes belonging to the same group are physically placed close to each other, node compromisation can be a success.

Computation complexity

Sensor nodes: This section compares the total computations performed for key generation in proposed scheme with schemes LARK, SHELL. In SHELL, sensor nodes perform two decryption for each administrative message received.

Cluster heads: In SHELL, for the distribution of keys generated by the EBS (exclusive basis system) matrix, CH requires four encryptions and four decryptions. The total computations performed can be represented by:

$$Computation_{SHELL} = [(r*2) + ((k+m)*4)] \quad (7)$$

If k = m = 7 and r = 2, the total computation is equal to 60 where k and r are number of administrative keys and gateways in each cluster. In each round of group re-keying, the cluster head calculate n secret shares for n sensor nodes and generate t degree polynomial; hence, computational complexity is O(n). Each secret share should be XORed with random number to prevent eavesdropping. The total computational overhead of CH is O(n) + ne, e denotes the XOR operation. Ordinary

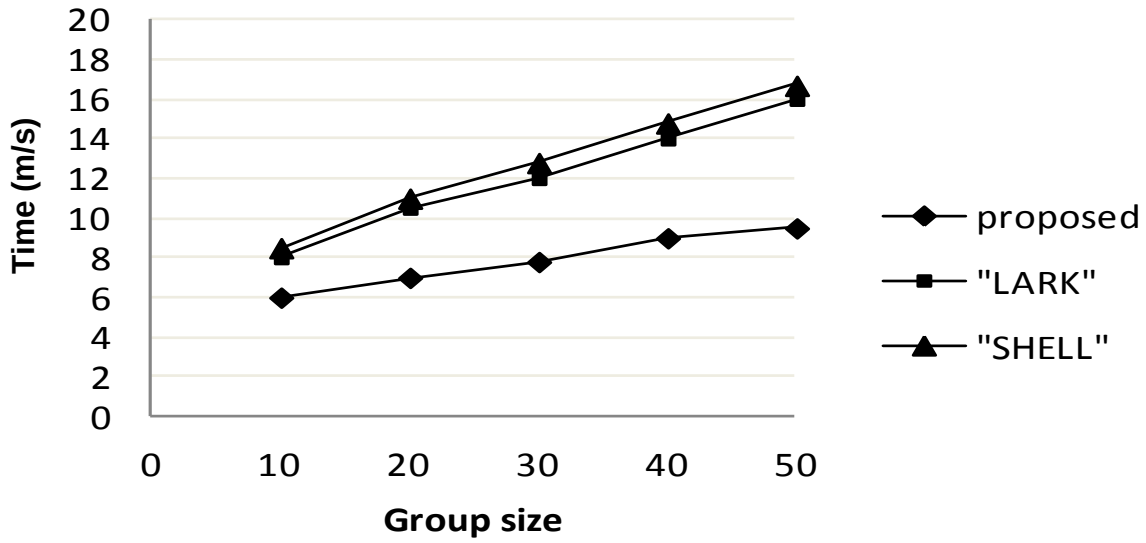

Figure 6. Time required for key establishment.

sensor nodes need one time XOR operation and generation of 't' degree polynomial. The operations that add to the computation overhead of LARK are decrypting the message received by the sensor node using SHA-1 cipher, validating the key authenticity for each key received by sensor node using a hash function, key is renewed when a sensor node enter or leave the group. When sensor node receives a message from the WSNC, it decrypts the message and checks the authenticity of the message. If authenticated, then the sensor node preprocesses the corresponding group key.

In the proposed scheme, each associated node generates the correlation key for authentication purpose. Also, the CH generates and distributes secret share used for generating the polynomial through which group key is generated by CNs. Hence, the computations performed for key generation is very low compared to the schemes LARK, SHELL. Figure 6 shows the time required for key generation by different schemes.

Key storage space

Sensor nodes: This section discusses the storage requirement of the proposed scheme and compares the storage requirement with existing schemes such as SHELL, LARK. In SHELL, each sensor node store three administrative keys K_{sg}, KS_{CH}, KS_{key}. Assume size of every key as 128 bits. Hence, the memory occupied in sensor node is 3*128 bits. Cluster heads store keys to communicate with its cluster members, other cluster heads and BS. Assume the values of 'k' and 'm' are 7, each and 'r' to be 2; further assumes the number of key values that SHELL store for key is 32. Total key maintained in the CH is (k + m + r)*32 = 16*32. In LARK, each sensor maintains two types of storage, storage for keys and storage for source codes. Key storage includes sensor-key and key ring for authentication. Moreover, LARK requires 23 KB of memory for storing source code of SHA-1. Each group is controlled by WSN controller (WSNC). WSNC need to store a sensor key, node identifier, key chain for each group member. In the proposed scheme, each sensor node store an association key of size 160 bit, a random nonce of size 8 bit and session key of size 8 bit.

Each cluster head store an association key of size 160 bit, a random nonce shared with BS of size 8 bit, a session key of size 8 bit. Figure 7 shows the memory requirement for different schemes. In the proposed scheme, each sensor node store 176 bit, a CH require 184 bit, BS require 168 bit. The total storage space is:

$$M_{total} = BS_{mem} + \text{No. of CH}*CH_{mem} + \text{No. of nodes}*SN_{mem} \quad (8)$$

Each node need to store one authentication key to maintain node authentication.

Conclusions

Group based sensor network applications is expected to grow rapidly. Therefore, it is necessary to ensure the secrecy of information communicated in group or cluster. The proposed scheme uses an authenticated cluster based key transfer protocol for group key generation and authentication. Here, confidentiality is ensured using a key transfer protocol based on Newton's divided difference interpolation. To prevent unauthorized access, group rekeying will be performed when a sensor node

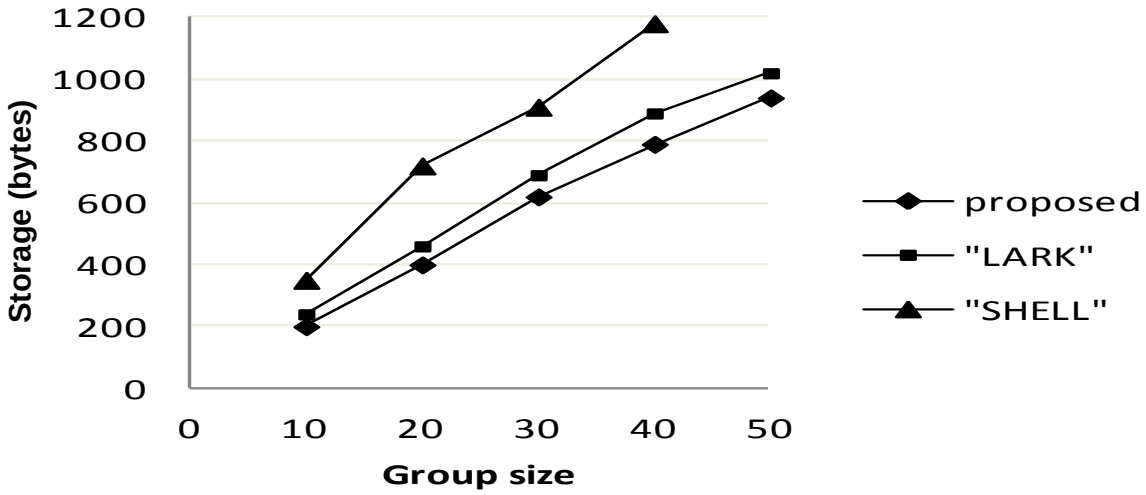

Figure 7. Comparison of memory requirement.

join or leave a cluster and for each session new group key will be used. Moreover, any information communicated between group members is secured and authenticated. The mechanism used for key generation is scalable with few messages. Also, this scheme is resilient to node compromise with reduced computation, communication and storage overhead.

REFERENCES

Amir Y, Kim Y, Nita-Rotary C, Tsudik G (2004). “On the performance of group key agreement protocols”. ACM Trans. Inf. Syst. Secur. 7(3):457-488.

Asem YM, Kara A (2006). A computationally efficient key-hiding based group re-keying scheme for secure multicasting. Int. J. Comput. Appl. pp. 65–73.

Chadha A, Liu Y, Das SK (2005). “Group key distribution via local collaboration in wireless sensor networks.”Proc. IEEE Sensor Ad Hoc Commun. Netw. pp. 46-54.

Chia-Yin L, Zhi-Hui W (2011). ”Secure key transfer protocol based on secret sharing for Group communication.” IEICE TRANS. Inf. Commun. Syst. Secur. E94-D:11.

Du W, Deng J, Han YS (2006). “Dynamic key management in sensor Networks”. Commun. Mag. 44:122-130.

Eltoweissy M, Heydari MH, Morales L, Sudborough IH (2004). “Combinatorial Optimization of Group Key Management.” J. Netw. Syst. Manag. 12(1):33-50.

GIANLUCA D, maria SI (2011). “Lark: A lightweight authenticated rekeying scheme for clustered wireless sensor networks.” ACM Trans. Embedded Comput. Syst. 10:4.

Heinzelman W, Chandrakasan HB (2002).” An application-specific protocol architecture for wireless micro sensor networks”. IEEE Trans. Wireless Commun. IEEE 802.11 Standard-1999 Edition 1:4.

Harn L, Lin C (2010). Authenticated group key transfer protocol based on secret sharing. IEEE Trans. Comput. 59(6):842–846.

Leonardo BO, Adrian F, Marco AV (2007). “SecLEACH - On the security of clustered sensor networks”. Sig. Process. 87:2882–2895.

Li AG, He J, Fu Y (2008). Group based intrusion detection system in wireless sensor networks. Comput. Commun. 31(18):4324-4332.

Manjeshwar A, Grawal D (2001). “TEEN: A protocol for enhanced efficiency in wireless sensor network”. In: Proceedings of the 15th Parallel and Distributed Processing Symposium, San Francisco, CA: IEEE Comput. Soc. pp. 2009−2015.

Manjeshwar A, Agrawal DP (2002).”APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks. Proceedings of the Parallel and Distributed Processing Symposium.

Wang Y, Ramamurthy B, Zou X (2007). “KeyRev: An efficient key revocation scheme for wireless sensor networks.” in ICC ’07: Proceedings of IEEE International Conference on Communications, Glasgow, Scotland, U.K.

Wei D, Kaplan S, Chan HA (2008). Energy efficient clustering algorithms for wireless sensor networks. Proceedings of IEEE Communications Society (ICC 2008) pp. 236–240.

Younis O, Fahmy S (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mobile Comput. 3(4):366–379.

Younis M, Ghumman K, Eltoweissy M (2006). “Location-aware combinatorial key management scheme for clustered sensor networks.” IEEE Trans. Parallel Distrib. Syst. 17:8.

Zhang W, Cao G (2005). “Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach.” Proceedings of IEEE INFOCOM.