http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (1): 28-39, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.28.39

Authenticated Group Communication to Mitigate Collusion Attack in Key Sharing

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

Abstract: Wireless Sensor Networks (WSNs) can be used in wide range of environment to handle various applications. During operation, sensor nodes are deployed in application specific area to sense data from surrounding environment. Sensor nodes in such environment are self organized. They lack physical protection and are vulnerable to various types of attacks. To protect the Sensor nodes from such vulnerabilities, the sensor nodes should own the security requirements such as authentication, confidentiality and integrity. One method of achieving confidentiality is through key management schemes. This article focus on group key management for clustered WSNs and proposes a group key management scheme based on secret sharing among the members of the group. Moreover, any information communicated within a group is secured and only authenticated members of the group can recover the group key. Unlike other schemes, the proposed scheme enhances the network security by resisting the effects of collusion among compromised nodes in group key recovery. Analysis and simulation results illustrate that the proposed scheme minimizes computation and communication overhead with low energy consumption for key establishment.

Key words: Group key, cluster-based, secret share, collusion, communication

INTRODUCTION

WSN is made up of several autonomous devices called sensor nodes. The sensor nodes are deployed in application specific region. Each sensor node senses the environment and collects the information from the field of interest (Radi *et al*., 2012). The sensed information has to be collected from the sensor nodes and the 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 (Dini and Savino, 2011). CH aggregates the data collected from its cluster and forward them to BS.

It is necessary to protect communication within a cluster, to make use of the advantages of cluster based communication in WSN (Wei *et al*., 2008). Security services such as confidentiality and authentication has to be considered for the design of secure group communication. Confidentiality is used to ensure the secrecy of sensed data. Authentication enables a node to verify the origin of data generated and ensure integrity of the data. In group communication (Li *et al*., 2008) confidentiality is used to ensure the secrecy of secret key shared between communicating parties. Confidentiality can be achieved through key management. One component of key management is the key used for encryption. The key should be securely shared between the communicating entities. There are number of traditional key sharing 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.

There are two types of group key sharing protocols (Chadha *et al*., 2005), key agreement protocols and key transfer protocols. In key agreement protocols (Amir *et al*., 2004) 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. The trusted entity generates

Corresponding Author: S.V. Annlin Jeba, Department of Computer Science and Engineering, C.S.I. Institute of Technology, Thovalai, Tamil Nadu, India

and transfer group keys secretly to all members in the group or cluster (Konstantinou *et al*., 2011). Secure group communication requires scalable and efficient group management 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 (Wang and Ramamurthy, 2007). When a sensor node leaves a cluster it must be prevented from accessing any further group communication. When a new communication is to be established, rekeying (Wang *et al*., 2007) will be performed to enhance key freshness in the group. The unique features of the proposed scheme are listed as:

- Energy efficient clustering mechanism is used
- The associated key assigned to the member nodes function as a measure of authentication
- Every group member need to register with the coordinator (CH or BS) to share the secret used in group key generation
- Uses a mathematical model for key sharing
- Reduce the effect of collision among the compromised nodes

RELATED WORKS

Energy efficient group communication technique is to be investigated to prolong the lifetime of WSN. Cluster based WSN architecture is one of the leading scheme for energy efficient communication. 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 to reduce the number of messages transmitted to BS.

LEACH: Low energy adaptive clustering hierarchy is the first clustering algorithm that was proposed for reducing power consumption in WSNs (Heinzelman *et al*., 2002). But LEACH is not applicable to networks deployed in large regions. HEED (hybrid, energy-efficient distributed) clustering is another distributed clustering approach (Younis and Fahmy, 2004). 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 (threshold sensitive energy efficient protocols) is suitable for time-critical sensing applications (Manjeshwar and Agrawal, 2001). This scheme is inappropriate for periodic monitoring of events. APTEEN (adaptive periodic threshold sensitive energy efficient sensor network protocol) (Manjeshwar and Agrawal, 2002): 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 study 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, 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 and Kara (2006) is a computationally efficient key hiding based group re-keying scheme in which keys are hidden in a numerical matrix and is send 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

sized 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, 2006) 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 are 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 collide 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 result in high communication overhead.

Lee *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. 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 centre 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.

Oliveira *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 members without the participation of BS. Overhead in SecLEACH is due to the factors such as message size and increased node CH distance.

Dini and Savino (2011) proposed a Lightweight authenticated rekeying scheme: LARK. LARK achieves security and scalability by using the mechanisms 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 results in communication overhead due to overlapping cluster. Also there is only one key server so each sensor nodes have to store their keys used for generating their group key.

PROPOSED SCHEME

This study proposed a reliable authenticated group communication to mitigate collusion attack in key sharing. The group key transfer protocol used in this scheme is based on a trusted entity. Here, the trusted entity, CH performs scalable and efficient group membership management with appropriate access control measures. Every time a membership change occurs, the group key is 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 is resilient to internal node compromisation, since any information shared among group members is secure and cannot be disclosed.

Scheme overview: The proposed scheme is divided into four phases:

- **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:** In the proposed scheme, members of the group (inter cluster, intra cluster) are authenticated by means of the associated key distributed by the BS. 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
- **Collusion detection phase:** When the CH receives key generation request from any of its members, it validates the request and then reply

Detailed procedure: The phases are explained in further detail below. For the sake of clarity and convenience description, important notations used are given in Table 1.

Table 1: Notations used

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

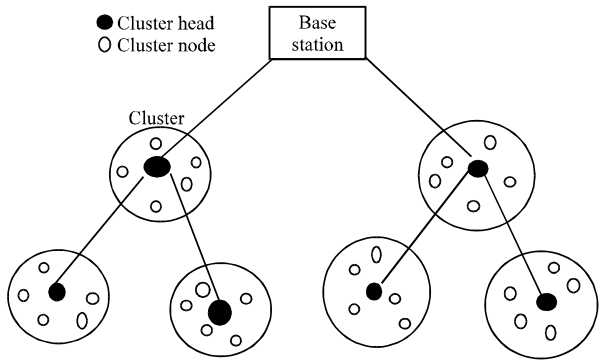

Fig. 1: Hierarchical cluster-based WSN

Cluster organization phase: After deployment of the sensor nodes in the area of interest, the sensor nodes are organized into clusters. The network architecture is depicted in Fig. 1. 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:

Step 1: Choose a number of desired clusters, k

Step 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

Step 3: Assign the remaining nodes to their closest CH. For each Ch_i, $i \in \{1,2, ..., k\}$ set the cluster C_i be the set of nodes in S that are closer to the cluster CH_i

Step 4: Construct the cluster in such a way that each cluster should contain minimum number of nodes

Step 5: Repeat step 3 in such away 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. The distance between CH_i and other sensor node within a cluster is given by $||CH_i-S_j||$, $j = 1 \ldots n$

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, trusted entities of the group should identify and authenticate their group members. Trusted entities are CH for intra cluster and BS for inter cluster communication. BS distributes Associated Key (AK) to CHs closer to the BS. 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 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 acknowledgment 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. A group key establishment

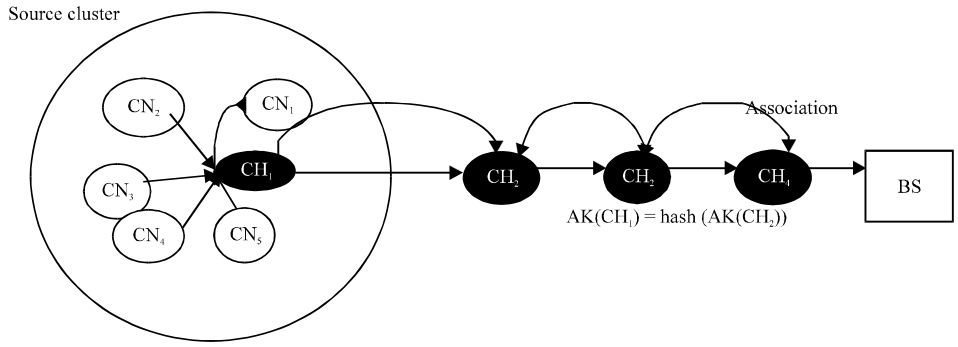

Fig. 2: Associated key (AK) represents the key generated by a node in association with another node using the key of the associated node, $AK(CH_1)$: Associated key (clusterhead$_1$), $H(AK(CH_2))$: Hash (Associated key (clusterhead$_2$)), BS: Base station, CN_i: Cluster node

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. In this scheme each group member should register with a trusted entity. The CH shares a secret with each cluster member. Moreover proposed scheme uses Newton's divided difference interpolation polynomial scheme for computing group 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:

- Intra cluster secret sharing (sharing between CH and other cluster members)
- 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:

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

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

- CH receives the message and get the random value R_i through exclusive XOR operation where

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

- 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 shares the secret $(x_i, y_i \oplus R_i)$ with each participating ordinary cluster nodes
- 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 intracluster 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 kth divided difference of f with respect to $x_1, x_2, \ldots, x_k$.

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

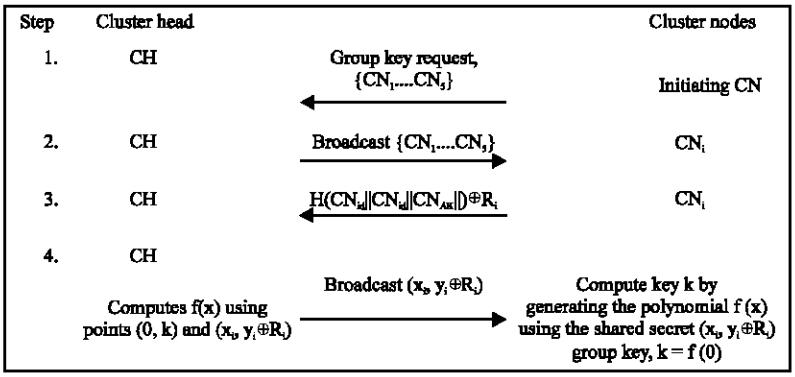

Fig. 3: Intra-cluster group key transfer

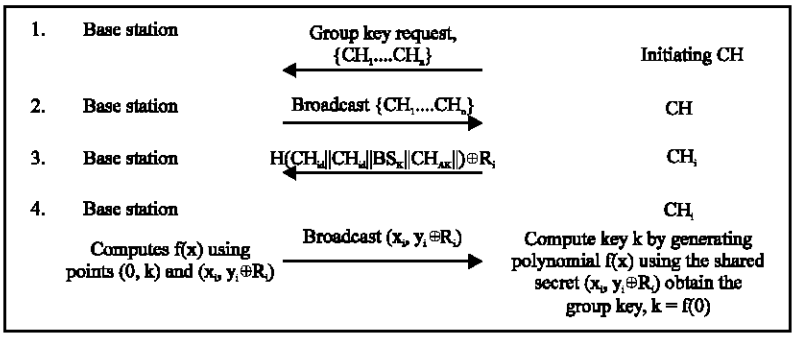

Fig. 4: Inter-cluster group key transfer

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

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

- BS receives the message and get the random value R_i through exclusive XOR operation where

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

- 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 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
- 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 intercluster 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 kth divided difference of f with respect to $x_1, x_2, \ldots, x_k$.

Collusion detection phase: When a CH receives a key generation request from any of its cluster members, it check whether the request is valid or not by means of the authenticated information maintained in the CH. If the request is valid then the CH initiates the key generation process otherwise reject the request. This process can be described through the Fig. 5. A subset of cluster members CN_1, CN_2 get compromise among themselves and try to discover new group keys for them. Hence, the initiating cluster member CN_1 send registration request along with

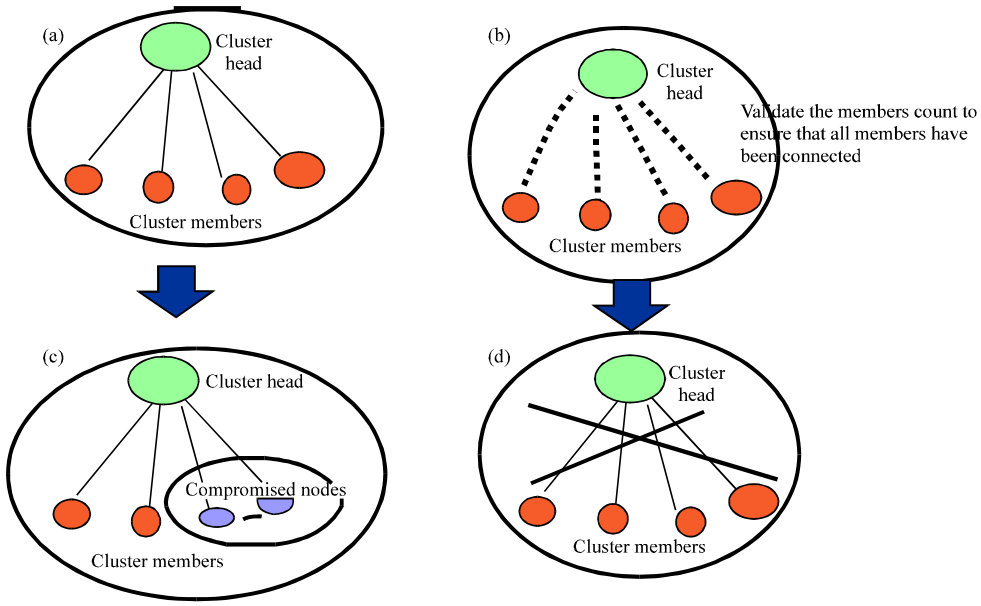

Fig. 5(a-d): A scenario for collusion detection within a cluster, (a) With its members, (b) CH authenticates its members, (c) Illegal sub group formation and (d) CH invalidate the communication

CN_2 as participating member of the group to the CH. The cluster head will not respond to the request send since in the proposed scheme CH regularly validate the count of its group members before initiating the communication in the group. Figure 5 describes the scenario of node compromisation within a group and how CH respond to the request send by compromised nodes within a group.

ANALYSIS AND DISCUSSION

Security analysis: This section discus about the possible attacks resisted by the proposed scheme.

Case 1: With stand outsider attack: Consider a situation where an adversary tries to share a group key by compromising one of the cluster members. In this case adversary was unable to generate the current group key used for communication within the cluster or group.

Though the adversary compromise a group member and get the group key stored in the group member, this group key cannot be used for future communication. Also using the old key new key cannot be generated due to the property of key independence. For each group communication one time secret key will be shared by the group member. The group key for future group communication can only be generated by the authenticated group member since the CH share the secret (x_i, $y_i \oplus R_i$) used for group key generation only with authenticated group member. Further, the adversary cannot get the random challenge used for registration of the compromised node with CH.

Case 2: Withstand replay attack: Assume a situation where an adversary eavesdrop the random challenge R_i of a cluster node CN_i during registration process. But the adversary cannot obtain the group key or secret share used for group key generation. Most of the previous schemes are not protected against replay attack. But the proposed scheme is resilient to replay attack.

An adversary CN_j eavesdrop R_i of a cluster node CN_i during registration with CH. Then the adversary sends R_i to the CH as if the message is from CN_i. The CH will not accept the registration since CH responds only to authenticate group member. Also the CH responds with secret share only for authenticated group member. Since adversary CN_j is not an authenticated cluster member, it cannot receive any communication from CH.

Case 3: With stand illegal subgroup formation attack: Assume a case where two or three members of a group collide among themselves to form subgroup and try to generate key for the subgroup. But subgroup formation cannot be a success in the proposed scheme.

A subset of cluster members CN_1, CN_2 get compromise among themselves and try to discover new group keys for them. Hence, the initiating cluster member CN_1 send registration request along with CN_2 as the participating member of the group to the CH. The cluster

Table 2: Comparison of functionality between proposed and related schemes

Schemes and measurement	SHELL	LARK	Proposed
Cluster architecture type	Disjoint cluster	Overlapping cluster	Hierarchical cluster
Deployment knowledge	Required	Not required	Not required
Dependency on IDS	High	High	Not Exist
Key renewal method	EBS (Exclusion basis system)	Mixing function	Polynomial expression
Communication round for secrecy	O(n)	O(log n)	O(2)
Scalability	High	Medium	Medium

LARK: Lightweight authenticated rekeying scheme for clustered WSNs, SHELL: Scalable, hierarchical, efficient, location aware light-weight scheme, SHELL is used in location aware combinatorial key management scheme for clustered sensor networks

head will not respond to the request send since in the proposed scheme CH regularly authenticate and validate the count of its group members before initiating the communication within the group. Thus illegal sub group formation and key generation for that subgroup can be prevented in the proposed scheme.

Comparison of functionality: In this section some comparison and analysis between the proposed and other related schemes based on their functionality are illustrated. In Table 2, the functionalities provided by each schemes are listed and the discussions are shown as follows.

The SHELL, LARK and proposed scheme possess cluster based architecture. In SHELL disjoint clusters are generated. But in LARK application specific clusters are formed. A node can be a member of more than one cluster and the clusters overlap each other. Moreover in SHELL physically close nodes share combination of keys. But in LARK and proposed scheme, key assigned is not related to the location of the nodes. In LARK and SHELL detection of compromised node is done through IDS (intrusion detection system) component included in the system. After detecting a compromised node, IDS forces the compromised node to leave the network. But the proposed scheme is highly resilient to node compromisation even though IDS is not included in this scheme. To achieve strong resiliency proposed scheme compute the session key using a mathematical based on a polynomial expression. In LARK and SHELL cryptography based functions are used for group key generation. SHELL can function correctly even in large network. But in LARK and the proposed scheme, if network size increases the number of trusted entities (KMS or CH) should also be increased. Thus the proposed scheme acquire more functionality for efficient group key management compared to the existing schemes.

Comparison of security: Comparison of security features between proposed and the existing schemes is listed in Table 3. Discussion shows that enhanced security can be achieved through the proposed scheme by means of high secrecy and strong resilience to node capture attack.

Table 3: Comparison of security features between proposed and related schemes

Schemes and measurement	SHELL	LARK	Proposed
Data authentication	No specific mechanism	Trigger-key	Associated key
Group key secrecy	Semi strong	Strong	Strong
Forward secrecy	Weak	Strong	Strong
Backward secrecy	Weak	Semi strong	Strong
Key refresh	Periodically	On demand	Each session need individual key
Resilience to node compromise	Low	Medium	Medium
Key independence	Low	Low	High
Security agent	Gateways, cluster head	Not Exist	Cluster head

LARK: Lightweight authenticated rekeying scheme for clustered WSNs, SHELL: Scalable, hierarchical, efficient, location aware light-weight scheme, SHELL is used in location aware combinatorial key management scheme for clustered sensor networks

In SHELL the group keys used for communication is generated by gateway nodes and cluster head using combinatorial formulation matrix. SHELL uses EBS (exclusion basis system) framework to perform rekeying within a cluster. This scheme reduces the number of message used for rekeying. Since nodes in a cluster receive the communication keys as combinatorial formulation the chance for node capture by collision is high. Another drawback of EBS framework used in SHELL is, communication messages used for rekeying is encrypted using the disclosed keys hence the secrecy of message exchanged is low. In LARK the group key is generated using a mixing function the components of mixing function include keys from key-chain and inverted key-chain. Backward security violation in LARK occurs when two or more nodes in a group get compromised and are physically placed close to each other. When the proposed scheme is compared with related schemes SHELL and LARK, it is found that in proposed scheme collision among compromised nodes would not affect the secrecy of group communication. Also the proposed scheme oppose forward and backward security violation since there is no relation between the previous and current group key generated when a node is added or removed from the cluster. Further due to the authentication mechanism used outside attackers cannot get back any information about the current group key used for communication. In the proposed scheme secrecy is maintained in any information communicated in the group hence eavesdropping cannot be performed.

Analysis of time complexity: The proposed scheme is compared with other schemes such as SHELL, LARK. It is assured that proposed scheme require minimum

Table 4: Compare time complexity between proposed and related schemes

Type of node	SHELL	LARK	Proposed scheme
Sensor node	$2T_{De}+T_{En}+T_H$	$2T_{De}+2T_H+T_{GK}$	$T_H+2T_{XOR}+T_{GP}+T_{GK}+T_r$
Cluster head	$4T_{De}+4T_{En}+T_{EBS}+T_{GK}$	Not exist	$T_H+2T_{XOR}+T_P+T_{GK}+T_{GP}$
Key management server	Not exist	$2T_{En}+(2*len)T_H$	Not exist

T_H: Time for hash computation, T_{GP}: Time to generate group polynomial, T_{GK}: Time to compute group key, T_{XOR}: Time to perform XOR operation, T_{en}: Time to encrypt a message, T_{de}: Time to decrypt a message, T_{EBS}: Time to compute the EBS matrix, T_P: Secret pair, T_{rand}: Time for random number generation, Len: Length of key chain

computation time for processing the group key. Table 4 shows node processing time of different schemes.

EXPERIMENTAL EVALUATION:

Experimentation is carried out to evaluate the security and efficiency of the proposed scheme with respect to related schemes. The network is simulated using NS2 simulator. In the simulation setting 500 nodes was randomly deployed in 1000×1000 m with same transmission range to all sensor nodes. Table 5 shows the simulation parameters used for the proposed scheme.

The experiment is run for varying number of compromised nodes and with clusters of varying size. The results obtained are analyzed to represent the performance of the proposed scheme. The related schemes LARK, SHELL make use of an Intrusion Detection System (IDS) to detect the presence of compromised node within the network. Practically IDS will not function well under all circumstances. If IDS fail to detect the existence of compromised node within the cluster, the counts of the compromised node get increased and the entire network gets captured. To overcome the drawbacks of the existing system, in the proposed scheme IDS is not used. Node compromisation in the proposed scheme is less likely to be performed since any communication within the network is confidential and authenticated.

Security evaluation: The objective of collision attack by an adversary is to attack individual nodes with an intend to recover and aggregate the keys that makes it possible to violate the secure communication in the network. Also collusion provides the probability to capture the entire network. The effectiveness of the proposed scheme against collusion attack is measured by two different metrics disclosure rate and distortion rate.

Disclosure rate: Disclosure or leakage rate represent the percentage of sensor readings exposed to compromised sensor nodes. This measure is used to measure the

Table 5: Simulation parameters

Parameter	Value
Network size	500 nodes
Simulation time	100 sec
Initial energy	1000 joules for network
Number of compromised nodes	10-60
Cluster size	60-100
Deployment	Random

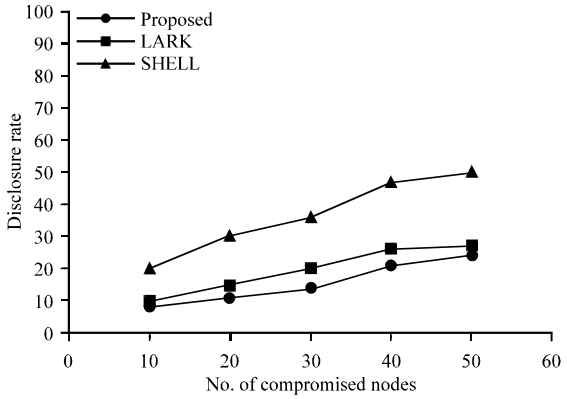

Fig. 6: Sensor data disclosure rate by compromised nodes

effectiveness of the security feature confidentiality of the proposed and related schemes during exchange of secured information within a cluster. One way of achieving confidentiality is through encryption.

Information distortion rate: Information distortion rate represent the percentage of sensor readings modified by compromised sensor nodes. This measure is used to measure the effectiveness of the security feature integrity of the proposed and related schemes during communication of secured information within a cluster.

Figure 6 shows the percentage of sensor data exposed by the compromised node to the sensor network during communication of confidential information within a cluster. Compared to LARK, SHELL the proposed scheme offer better confidentiality since any data communicated is secured and authenticated. In SHELL compromised sensor node can be determined and evicted only through IDS and practically the operation of IDS is not perfect. The compromised nodes are not permanently forced to leave the network. The presence of compromised nodes tries to compromise other uncompromised nodes. The evicted nodes have no effect if all the administrative keys are known to the attackers. But mechanisms other than IDS can operate well and achieve maximum benefit. In LARK confidentiality is achieved through one way hash function. SHA1 is used for performing hash. The strength of SHA1 against collusion resistance is low. Hence, the possibility of

broking confidentiality is high. If broken, more information can be exposed. In the proposed scheme IDS is not used and evicting of compromised node can be done by rejecting messages from compromised sensor nodes to CH or not responding to the messages received from compromised sensor node.

Figure 7 shows the information distortion rate of sensor node communicated within the cluster. The sensor data is generated by uncompromised sensor node and modified by compromised sensor node. In related schemes such as LARK, SHELL data security is achieved by encryption of data using the key generated within a cluster. If more compromised nodes are there in a cluster retrieving the secret key through compromised node can be done faster hence, security the data communicated can be broken and false information can be injected to the information on transit. Also in Lark no specific mechanism for authentication is used. The key chain is used as authentication measure. If the hash function is broken, authentication would not be secure anymore since the compromised sensor node will modify the sensor data communicated within the cluster. But in the proposed scheme node authentication and data authentication measures are very efficient and strong integrity can be achieved compared to the existing scheme. Also, if a compromised node is detected it will be permanently.

Efficiency evaluation: The performance of the proposed scheme is evaluated in terms of energy consumption and time consumption for key establishment.

Energy consumption: The energy performance of the proposed scheme has been evaluated by analysing the energy consumption for key renewal by proposed scheme with related schemes LARK, SHELL. Figure 8 shows the energy consumed for key renewal by the proposed and related schemes of different cluster sizes. In the proposed scheme energy consumption increase gradually with increase in group size, since the function of key computation is assigned to individual member nodes. Moreover in the proposed scheme the number of messages communicated within the cluster to enhance security is less. Hence less communication overhead and low energy consumption occur in the proposed scheme. But in SHELL number of exposed administrative keys gets increased with the increase in number of compromised node. Hence more energy is consumed for key renewal which includes the energy spent for cluster reorganization, administrative key generation and administrative key distribution.

Time consumption: Time consumption measures the time required by the sensor node to renew the key used to establish communication within a group at present. Unlike other schemes proposed scheme does not use a cryptographic technique for key establishment. A simple mathematical model with minimum computation is used for key establishment. Figure 9 shows the time

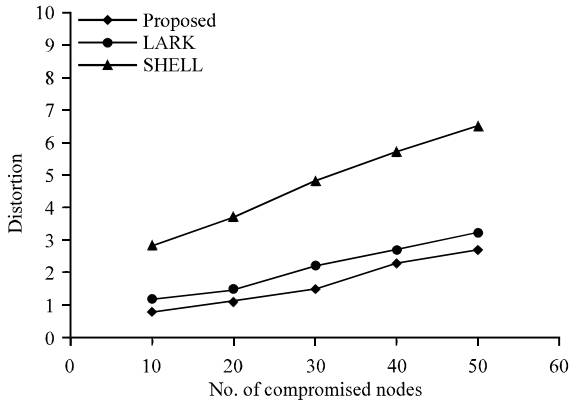

Fig. 7: Sensor node information distortion rate by compromised nodes

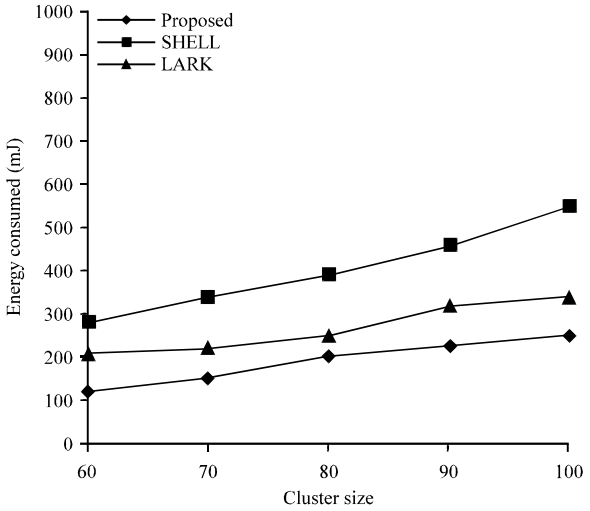

Fig. 8: Energy consumption of different schemes for key renewal

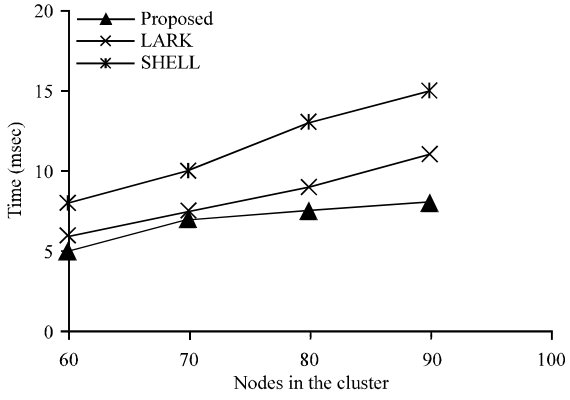

Fig. 9: Time consumption for key renewal

required for key renewal with different cluster sizes. Time consumption for key renewal is inversely proportional to group size.

CONCLUSION

Group based sensor network applications tend to grow in large extend from health care to warfare. Hence, it is necessary to ensure secrecy of information communicated within the group or cluster. One method of achieving secrecy is through key management. Security through key management is by using keys for encryption which should be securely shared within the group. In the proposed scheme, group key management operations are distributed among all members in the group. Further, the proposed scheme reduces the effect of collusion among compromised node to recover the group key. Moreover proposed scheme includes an efficient authentication mechanism which prevents unauthorized nodes to join group communication. Security analysis illustrate that the proposed scheme is resilient to outsider attack, replay attack and collusion attack within the group.

REFERENCES

Amir, Y., Y. Kim, C. Nita-Rotary and G. Tsudik, 2004. On the performance of group key agreement protocols. Trans. Inform. Syst. Secur., 7: 457-488.

Asem, Y.M. and A. Kara, 2006. A computationally efficient key-hiding based group re-keying scheme for secure multicasting. Int. J. Comput. Appl., 28: 65-73.

Chadha, A., Y. Liu and S. Das, 2005. Group key distribution via local collaboration in wireless sensor networks. Proceedings of the 2nd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, September 26-29, 2005, California, USA., pp: 46-54.

Dini, G. and I.M. Savino, 2011. Lark: A lightweight authenticated rekeying scheme for clustered wireless sensor networks. ACM Trans. Embedded Comput. Syst., Vol. 10. 10.1145/2043662.2043665

Eltoweissy, M., M. Moharrum and R. Mukkamala, 2006. Dynamic key management in sensor networks. Commun. Magaz., 44: 122-130.

Eltoweissy, M., M.H. Heydari, L. Morales and I.H. Sudborough, 2004. Combinatorial optimization of group key management. J. Network Syst, Manage., 12: 33-50.

Harn, L. and C. Lin, 2010. Authenticated group key transfer protocol based on secret sharing. IEEE Trans. Comput., 59: 842-846.

Heinzelman, W.B., A.P. Chandrakasan and H. Balakrishnan, 2002. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun., 1: 660-670.

Konstantinou, E., G. Kambourakis and S. Gritzalis, 2011. A survey on cluster-based group key agreement protocols for WSNs. IEEE Communi. Surveys Tutorials, 13: 429-442.

Lee, C.Y., Z.H. Wang, L. Harn and C.C. Chang, 2011. Secure key transfer protocol based on secret sharing for group communication. IEICE TRANS. Inf. Communic. Syst. Sec., E94-D: 2069-2076.

Li, A.G., J. He and Y. Fu, 2008. Group based intrusion detection system in wireless sensor networks. Comput. Commun., 31: 4324-4332.

Manjeshwar, A. and D.P. Agrawal, 2001. TEEN: A protocol for enhanced efficiency in wireless sensor network. Proceedings of the 15th International Parallel and Distributed Processing Symposium. April 2001, IEEE Computer Society, San Francisco, CA., pp: 2009-2015.

Manjeshwar, A. and D.P. Agrawal, 2002. APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. Proceedings of the 16th International Parallel and Distributed Processing Symposium, April 15-19, 2002, Fort Lauderdale, FL., USA., pp: 195-202.

Oliveira, L.B., A. Ferreira, M.A. Vilaca, H.C. Wong, M. Bern, R. Dahab and A.A.F. Loureiro, 2007. SecLEACH-on the security of clustered sensor networks. Signal Process., 87: 2882-2895.

Radi, M., B. Dezfouli, K. Abu Bakar and M. Lee, 2012. Multipath routing in wireless sensor networks: Survey and research changes. J. Sensors, 12: 650-685.

Wang, Y. and B. Ramamurthy, 2007. Group rekeying schemes for secure group communication in WSNs. Proceedings of the IEEE International Conference on Communications, June 24-28, 2007, Glasgow, pp: 3419-3424.

Wang, Y., B. Ramamurthy and X. Zou, 2007. KeyRev: An efficient key revocation scheme for wireless sensor networks. Proceedings of IEEE International Conference on Communications, June 24-28, 2007, Glasgow, Scotland, UK., pp: 1260-1265.

Wei, D., S. Kaplan and H.A. Chan, 2008. Energy efficient clustering algorithms for wireless sensor networks. Proceeding of the IEEE International Conference on Communications Workshops, May. 19-23, Beijing, China, pp: 236-240.

Younis, M., K. Ghumman and M. Eltoweissy, 2006. Location-aware combinatorial key management scheme for clustered sensor networks. IEEE Trans. Parallel Distrib. Syst., 17: 865-882.

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

Zhang, W. and G. Cao, 2005. Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach. Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, March 13-17, 2005, Miami, FL, USA., pp: 503-514.