I.J. Computer Network and Information Security, **2014, 8, 9-18**
Published Online July 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.08.02

Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks

Abdoulaye Diop, Yue Qi, Qin Wang
University of Science and Technology Beijing, School of Computer and Communication Engineering, Beijing, China
Email: adiop.ustb@gmail.com, qiyuee@ustb.edu.cn, wangqin@ies.ustb.edu.cn

Abstract—Research in Wireless Sensor Networks (WSNs) has made a significant progress recently, especially the area of key management, which plays a central role for protecting group communication in sensor networks. In sensor networks, the data are crucial and have to keep secrecy in data communication. To achieve data confidentiality, adversary should not have access to the group communication. Therefore due to the limited memory resources and energy constraints of sensor nodes, reducing the communication and storage overhead, and improving the resilience against the node capture attack become a must.

In this paper we propose An Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks (EGKMST). The proposed scheme considers a hierarchical cluster structure of sensor network and adopts the pair-wise key management and group key management based on threshold key cryptography to generate and to distribute the keys efficiently within a cluster and updates periodically keys. By this way EGKMST provides continuous transmission security and avoids dangerous attacks from malicious nodes and mitigate the node compromise attack in WSNs communication. The security and performance analysis illustrate that EGKMST scheme achieves the requirement of group communication and provides efficient security with low communication cost, low memory overhead and energy saving compared with some existing key management schemes.

Index Terms—Wireless Sensor Network, Symmetric Key Management, Security, Attacks, Cluster.

I. Introduction

A Wireless sensor network (WSN) consists of a number of micro devices called sensor nodes with low cost, low energy consumption which are distributed autonomously in an area for purpose of monitoring. WSNs have lot of applications in military, health and other industrial sectors.

In WSNs security, data confidentiality is one of the most important requirements. Further to achieve this requirement, adversary should not have access to the group communication. Therefore, due to the limited memory resources and energy constraints of sensor nodes. [1, 2](ref. Fig. 2), reducing the communication cost, the storage overhead and also improving the resilience against the node capture attack become a must. Recently several enhanced secure cluster based routing protocols have been proposed in literature [20, 26, 31, 33, 34] to achieve both security and efficiency for WSNs. Figure 1 shows the basic security requirements of WSNs. Furthermore these protocols have their own advantages, but most of them are vulnerable to node compromise [10] and provide high communication and memory cost.

In this chapter we propose An Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks (EGKMST). The proposed scheme considers a hierarchical cluster structure of sensor network [11]. EGKMST adopts pair-wise key management and group key management based on threshold key cryptography [12, 13] to generate and to distribute the keys efficiently within a cluster and updates periodically keys. By this way EGKMST provides continuous transmission security

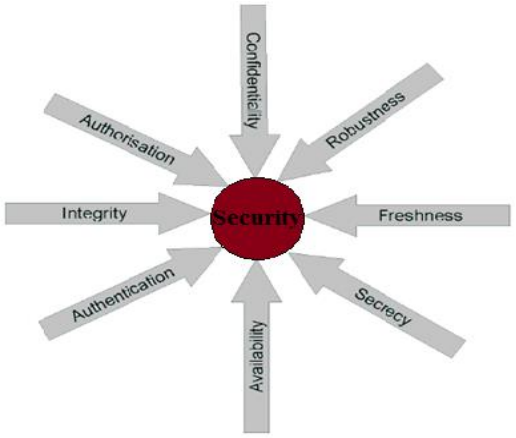

Fig 1. Basic security requirements in WSNs

and avoids dangerous attacks from malicious nodes and mitigate the node compromise attack in WSNs communication [10, 27, 28].

The rest of the paper is organized as follows. Section 2 describes the related work. In Section 3 and section 4 we present the network model and the proposed key

management scheme in details. Session 5 states the security and performance analysis of our scheme. Finally, we conclude our work and present some future research directions in section 6.

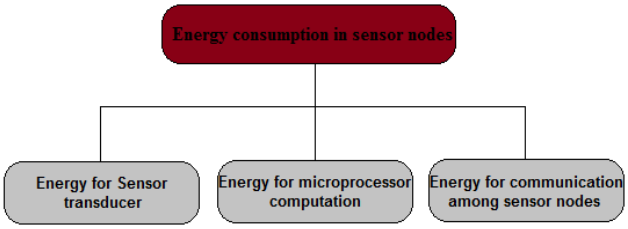

Fig 2. Sensor nodes energy consumption.

II. Related Work

Key management plays a central role for protecting communication in wireless sensor networks. In the area of key management, the group key is one of the fundamental security mechanisms that are able to provide secure group communication [29]. Therefore, the cluster based sensors networks behaves better in performance and reliability than traditional flat WSNs (FSNs) as [36]. Several key distribution and management schemes have been proposed in WSNs. For securing LEACH (Low-Energy Adaptive Clustering Hierarchy) presented by Heinzelman et al. [2], Zhang et al. proposed RLEACH [3] a secure routing protocol for cluster-based WSNs, using group key management to solve the problem of secure LEACH. Using improve random pair-wise key management scheme, RLEACH resists to different attacks such as selective forwarding, sinkhole attacks. Otherwise RLEACH fails against node capture attack. Jolly et al. proposed low-energy key management protocol LEKM [16]. Sensor nodes communicate only with CH within the same cluster. Further, LEKM used group keys to secure the communication between two cluster heads. Otherwise the main drawback of LEKM is that all the keys stored in sensor nodes within a cluster are compromised, once the cluster head is captured. Zhang and al [21] focus on reducing the communication overhead and storage cost of sensor nodes and propose a cluster-based group key management scheme for WSNs, they employ the threshold cryptography [12,13] and to solve the node isolation problem. The weakness of this scheme is that the communication security within a cluster is affected, once a CH is captured. This scheme also doesn't provide secure communication between the sink node and cluster heads. Based on Shamir's (t, n) secret sharing (SS), Harn and Lin (2010) [35] proposed an authenticated group key distribution protocol. This scheme need a key generation center to construct and transfer the group key which increases the overhead required for the system implementation. However, KGC is susceptible to single point failure. This scheme cannot be used for real life application. Tubaishat et al [14] proposed a Secure Routing Protocol for Sensor Networks SRPSN. In this scheme, a group key management scheme is proposed, which contains group communication policies, group membership requirements and an algorithm for generating a distributed group key for secure communication. Every sensor node contributes its partial key for computing the group key. One drawback associated with this protocol is that there is no authentication mechanism. Therefore, SRPSN fails against some attacks like spoofing, altering, replaying. If the adversary uses the Sybil attack, the problem will be more severe. The malicious node can also become a sinkhole. Y. Cheng and D. Agrawal proposed an Improved Key Distribution Mechanism IKDM [11] based on hierarchical network architecture and bivariate polynomial-key pre-distribution mechanism. In IKDM, Only two pair-wise keys are preloaded in each sensor node to reduce the key storage overhead. Otherwise, one weakness of this approach is that once a cluster head is captured, all the keys stored in sensor nodes in that cluster will be compromised. Therefore, it is required either to replace the sensor nodes in a cluster or replace a compromised cluster head in that cluster. Yin and Madria [15] proposed a Secure Routing Protocol for sensor networks SecRout to provide security against attack from compromised nodes in sensor networks. SecRout uses two types of keys: the master shared key used between the sink and CHs, and the cluster key among the clusters to encrypt the message. Therefore, SecRout can greatly save the energy. However SecRout fails to mitigate the wormhole attack and don't provide privacy. EECBKM [4] Energy-Efficient Cluster Based Key Management is a cluster based technique for key management in WSNs. The EBS key set contains the pair-wise keys for intra-cluster and inter-cluster communication. Results have shown that EECBKM reduces node-capture attacks. However fails to mitigate selective forwarding and wormhole attacks. Ibriq and Mahgoub [5] proposed a secure hierarchical energy-efficient routing protocol SHEER, which provides energy-efficient and secure communication. SHEER mitigates hello flood attack, sybil attack. However SHEER fail to protect the network from selective forwarding attacks. Gawdan et al. [9] proposed a Novel Secure Key Management module for Hierarchical Clustering WSNs NSKM. In NSKM, there are three categories of keys; pre-deployed keys, network generated keys and the BS broadcasted keys. NSKM module is energy-efficient, has strong flexibility against susceptible attacks on WSNs. AKM [25] is an Authenticated Key Management scheme for hierarchical networks based on the random key pre-distribution. Security is provided by using two kinds of keys. AKM provides confidentiality, global and continuous authentication of nodes in the network. However, if adversary re-enters the compromised node into the network before refreshing the current network key, the resiliency of AMK scheme will be same as given in Eschenauer et al. [18].

To improve Eschenauer and Gligor[18] scheme, Chan et al. propose the q-composite key pre-distribution [19] to improve the network resilience against node capture attacks. Two sensors need to share at least q common

keys to setup a pair-wise key between them. SecLEACH [7] is an improvement of SLEACH [6]. Hence, SecLEACH shows how a random key pre-distribution can be used for secure communication in cluster-based protocols. However GS-LEACH [22] and SecLEACH present some security vulnerabilities caused by the random key pre-distribution scheme and are also vulnerable to key collision attacks. Wu et al. proposed a protocol based on LEACH protocol SS-LEACH [8], considering routing security and network lifetime. SS-LEACH protocol strongly improves the energy-efficiency However SS-LEACH doesn't provide message integrity and fails against sinkhole and wormhole attacks.

To overcome the limitations of current key distribution and management schemes, we propose An Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks (EGKMST). Based on the hierarchical network structure and symmetric key mechanism, EGKMST uses pairwise key management and group key management to provide efficient security and resilience against dangerous attacks with low communication cost, low storage overhead and energy savings.

III. Network Model

The proposed scheme considers a hierarchical cluster structure of sensor network [11] [17], as illustrated in Fig. 3.

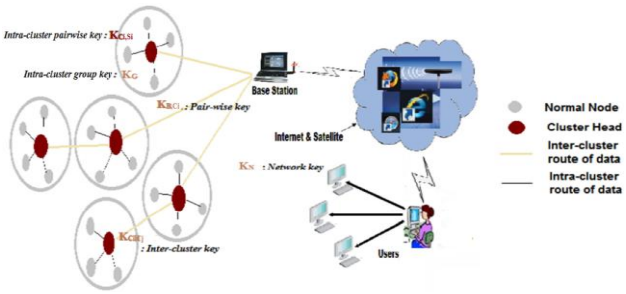

Fig 3. Proposed scheme architecture.

- BS is considered trustworthy with unlimited resources and is located in a safe place. BS has authentication system for any node in the network [23], a node member table of all nodes in the network and an intrusion detection system.
- Cluster head (CH) is responsible for collecting data within a cluster and sends to the BS.
- Sensors nodes (SNs) collect information of surrounding environment and transmit to the CH.

Initially, sensor nodes keep stationary after deployment during the network operation. To distinguish between them, each node has a unique id with enough length.

The proposed technique use LEACH [2] to randomly join a cluster. Sensors nodes choose their cluster head according some parameters such as the strongest signal received [2, 24]. Fig 2. shows the flow chart of LEACH protocol. The present scheme is static, sensors nodes cannot act as a CH and there is no communication between sensors nodes. We assume that CHs can communicate each other if CH is located far from the BS. In this case, CH sends the aggregated sensing data to the relay CH near the BS to save energy.

In this network model, each exchanged message has a timestamp that guarantee the freshness of information. We also consider a minimum time "Tm" after deployment, in which a node cannot be compromised.

In this proposed key management technique the descriptions of the notations used are listed in Table 1.

TABLE I. Type Sizes for Camera-Ready Papers

S. No	Notation	Description
1.	id_{SNi}	Identification Number of node i
2.	id_{CHi}	Identification Cluster Head i
3.	id_{BS}	Identification Base Station
4.	K_N	Network key
5.	K_{pair}	Pairwise key
6.	K_{Ci-Si}	Intra-cluster pairwise key
7.	K_{Group}	Intra-cluster group key
8.	$K_{Ci,Cj}$	Inter-cluster key
9.	$E_K(M)$	Encryption of M with symmetric key K
10.	H ( )	One-way hash function
11.	$MAC_K()$	The message authentication code of message M using symmetric key K
12.	$\oplus$	Bit wise XOR operation
13.	N	Nonce

IV. The Proposed Key Management Scheme

A. Procedure of threshold scheme based on Langrange

In this subsection, we briefly introduce the threshold cryptography [12, 13] used in key management. Therefore to perform cryptographic operations, an *(n, t)* threshold scheme allows n parties and only any t parties can jointly perform key discovery, whereas *(t − 1)* parties cannot derive any information.

For example Shamir's *(t, n)* [12] threshold scheme based on Lagrange interpolating polynomial consider a chosen secret D and chose t degree polynomial

$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$ to store D into n pieces.

Where a0 = D and (f(1), f(2), ・ ・ ・ , f(n)) are the n pieces of secrets.

The coefficients of *f(x)* can be derived by interpolation using t points from the n pieces and so calculate the secret $D = a_0$. Otherwise cooperation of t − 1 points cannot reconstruct the secret D.

B. Our proposed protocol

Based on the principle of symmetric key cryptography and threshold key cryptography our protocol uses four types of keys: the network key (K_N), the pairwise key (K_{pair}), intra-cluster pairwise key (K_{Ci-Si}), the intra-cluster group key (K_{Group}). Therefore EGKMST involves these following phases:

1. Initialization phase:

Before the deployment, all legitimate nodes are preloaded with one network key K_N. Note that K_N will be used by BS and all nodes in the network during the cluster formation phase and for authentication process. In addition, initially during this phase BS determines groups of nodes and generates for each group a polynomial *f(x ,y) of degree 2t.*

Therefore each node is loaded by a unique secret

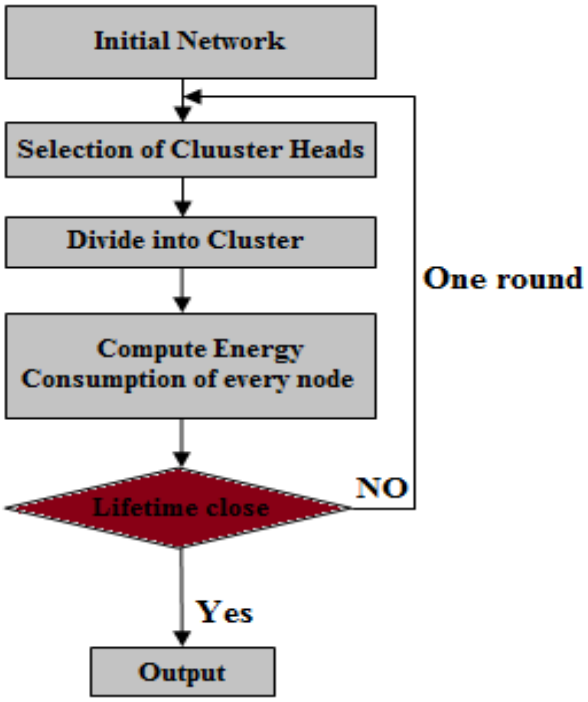

Fig 3. Flow chart of LEACH protocol.

shared:

$$f(id_{SNi}, y) = \sum_{i,j=0}^{2t-1} e_{ij}(idSNi)^i y^j \mod (P) = h_{idSNi}(y), \quad (1)$$

Where id_{SNi} is the node identifier and *P* is the random prime number *(e_{ij} are less than P).*

2. Pairwise key establishement:

After the deployment and cluster organization phase. Clusters are formed based on cluster selection algorithms and on the number and type of nodes [2, 24]. BS needs to establish pairwise key with each cluster head to secure communication between them.

Algorithm-1: Pairwise key Management:

Step 1. Key Generation Request Phase

1. *The CH first time sends a pairwise key generation request (KREQ) to the BS by inserting its ID and encrypting message using K_N.*

CHi →BS: KREQ {id_{CHi},id_{BS}, $EK_N(M||N)$, $MACK_N(M||N)$}

Data integrity and authentication are providing by MAC, the timestamp N avoids message replay attack. M is the cluster head's message M= ($id_{CHi}|id_{BS}|K_N$).

Step 2. Validation and Key Generation

2. *Upon receiving the CH information, the BS authenticates M and verifies the MAC:*
3. *if (authentication is successful) then*
4. *BS generates the pairwise key (K_{pair})*
   $K_{pair} = HK_N(id_{CHi} \oplus id_{BS} \oplus N)$
5. *else (ClusterHead not valid) then*
6. *BS drop Msg*
7. *end if*
8. *Base station encrypts M and K_{pair} using network key in an authentication response (KREP) and sends it to cluster head.*

BS →CHi: KREP {id_{CHi}, id_{BS},$EK_N(M||N||K_{pair})$, $MACK_N(M||N)$}

9. Stop.

3. Intra-Cluster Pairewise Key Management KCi-Si:

This phase describes the intra-cluster pairwise key establishment between cluster members and CH in the same cluster. First the sensor node SNi sends a key generation request to its CH. Upon receiving the SN's information, CHi authenticates nodes SNi and sends the identity list of all node members in the cluster (id_{List}) to the BS. BS computes the intra-cluster pairwise key $K_{Ci\text{-}Si}$ using one-way hash function and sends it to the CH with an authentication response message. Therefore CHi authenticates BS, decrypts the message and send the news keys $K_{Ci\text{-}Si}$ to all cluster members .The cluster members (CMs) willing to trust the CH, will use $K_{Ci\text{-}Si}$ as the shared key between CHi and CMs.

Algorithm-2:Intra-Cluster pairwise key Management

1. SNi → CHi : id_{SNi},id_{CHi} $||EK_N(M|N)||$ $MACK_N(M|N)$

2. CHi → BS:id_{CHi},id_{BS} $||EK_{pair}(M|N||id_{List})||K_{pair}(M|N)$

Where idList = {idSN1,idSN2, ⋯⋯ ,idSNk-1}

3. BS → CHi: id_{BS},id_{CHi} || $EK_{pair}(M|N|K_{Ci,Si})$ || $MACK_{pair}(M|N)$

4. CHi → SNi : $id_{CHi}||EK_N(M|N\ K_{Ci,Si})$ $||MACK_N(M|N)$

k : is the number of node in the cluster.

It is worth noting that when CH_1 is located far from the BS, CH_1 uses the relay CH_2 along the path to communicate with BS. In this case the BS generates $K_{Ci,Cj}$

named Inter-cluster key for secure communication between CH_1 and CH_2. Thus CH_1 uses this key to communicate with CH_2 in a secure way.

4. Intra-cluster group key establishement:

The intra-cluster group key is the shared key between the CH and cluster members within a cluster, protecting their communication based on shared secret. This key generation process is as follow.

Firstly, the CHi send broadcast message to *t* member nodes SNi within a cluster to request their corresponding secret shares.

Once received the request message, SNi authenticates CHi and returns its personal secret shares $h_{idSNi}(y)$.

$$SNi \rightarrow CHi : h_{idSNi}(y)$$

if match // CH success to obtain t personal secrets where t is the threshold value.

CH reconstructs K_{Group} using Lagrange Interpolation polynomial by collecting a threshold number of t keys.

The CH can derive the group key from $K_{Group} = h(0)$.

Then the CH establishes a communication more secure with cluster members within a cluster by using the intra-cluster group key.

5. Key updating phase:

In this scheme the network key K_N is updated periodically. Further, BS generates and sends the new network key K_{N+1} to CHi encrypting with K_{pair}. CHi authenticates the message, decrypts and broadcasts the network keys to legitimate cluster members.

The intra-cluster pairwise keys can also be refreshed periodically. In this case BS using the hash function and the current intra-cluster pairwise key, generates a new key. The messages are encrypted with K_{pair} and sent to CHi. CHi authenticates the message and transmits the new keys to its cluster members, encrypted with the current key $K_{Ci\text{-}Si}$ only known by the legitimate cluster members.

For the intra-cluster group key, the BS initiates rekeying by sending new secret shares to sensor nodes, hence CH after obtaining t personal secrets key from cluster members within a cluster, can compute the new key to improve key updating and to secure group communication..

V. Security And Performance Analysis

A. Scalability:

1. Node deletion

In WSNs, it is necessary to preserve the shared keys secrecy when a node is compromised, thus avoid the number of compromised nodes reached a critical value. In our EGKMST scheme, upon identifying a compromised sensor node, CH broadcasts a notification to its cluster members and removes the compromised node from its cluster member table.

If a CH is compromised, a re-clustering of cluster member of the compromised CH among the remaining CH needs to take place. In this case, BS informs its cluster members and other CHs. Cluster member of the compromised CH are distributed among other uncompromised CHs. For cluster organization, the clustering algorithm as discussed in [2, 24] is used. Afterward BS initiates the key update mechanism, however nodes discards its currents keys and uses a new network key and cluster key for future communication.

2. Node addition

If a new node is added in the network, the BS after authentication process assign the new node in a group and loads it with the unique secret shared $h_{idSNi}(y)$, the current network key and the intra-group key. The BS notifies the CHs about the new node's arrival. Then, CHs send an advertisement message adv. Once receiving requests from CHs, new node selects one of the CHs as its own CH, based on some parameters such as the strongest signal received from a CH [2]. Then new node sends to the CH an encrypting join request message including its ID and the CH's ID. Afterwards, the selected CH establishes a intra-cluster pairwise key with the new node.

However the BS initiates rekeying by sending new secret shares to node cluster members of the new node. Thus each node's, including the new node obtain a unique secret shares enhancing key refreshness and securing group communication and process continues.

B. Robustness:

EGKMST scheme adopts the concept of symmetric key management and threshold key cryptography. Further, the present group key management scheme satisfies these following properties.

Theorem 1: EGKMST provides basic security requirements and is secure against spoofed, altered and replayed packets attacks.

Proof: In these attacks, adversary alters, spoof or replay the routing information [10, 28]. It can also reply routing information. As a result, it could increase the delay. Further, before message transmission, encryption is performed to secure the communication with the help of one way hash function, used to provide authentication and message integrity.

In EGKMST, each cluster members encrypts information using the intra-cluster pairwise key $K_{Ci\text{-}Si}$ and the intra-cluster group key K_{Group}, avoiding eavesdropping attacks. Therefore only legitimate CH that owns $K_{Ci\text{-}Si}$ key and K_{Group} can decrypt the message. EGKMST provides freshness using time interval, time-stamps and nonce. The nonce N is very important since it prevents a replay attack and ensures the integrity of the message. Further to know the origination of the message for further action, BS and nodes check the id which is attached to the message. To prevent a malicious node to

attempt keys establishment, the BS authenticate CH by verifying the MAC calculated using K_N. Since K_N is only known by the BS and legitimate nodes. The MAC ensures the data integrity and authentication of sensing data and avoids the Spoofing attacks.

Theorem 2: EGKMST provides a secure intra-cluster group key distribution.

Proof: EGKMST exploits a threshold key cryptography to protect the security of system group key K_{Group} [13]. Therefore it is noting that the communication cost increases a little bit, since only cluster heads construct the group key polynomial. Moreover adversary can compromise the polynomial $h_{idSNi}(y)$ only when: (i) for a given time, more than t nodes in different cluster are compromised, or (ii) if a sensor node is captured and t or more of its cluster members are also captured.

Theorem 3: EGKMST mitigates sinkhole and wormhole attacks, two attacks which cannot be mitigate by most schemes in cluster based WSNs.

Proof: In Sinkhole attack, attacker presents himself with high capability resources, by which announces a short path to destination to attract packets and then may drop them [30]. Otherwise, adversary launch wormhole with tunneling mechanism to establish it between entities by confusing the routing protocol [30].

Regarding our key management scheme, an adversary does not possess all the cryptographic keys required for achieving node authentication with BS and the corresponding CH. We consider that the attacker requires a fixed amount of time to compromise the node, hence in our scheme, keys are periodically refreshing.

Table II. A Comparative Overview Of Representative Secure Hierarchical Routing Protocols For WSNs

Protocol Name	*Ref*	*Cryptography Scheme*	*Key distribution and Management Scheme*	*Authentication Scheme*	*Storage Load*	*Comm. Load*	*Scalability*	*Robust-ness*	*Connectivity*	*Energy Efficiency*
RLEACH	[3]	Symmetric key cryptography	Improved Random pair-wise key management (IRPK)	Authentication is achieved via IRPK	High	Medium	Good	Good	Probabilistic	Medium
EECBKM	[4]		EBS-based key Management schemes	Via Key Management	Low	Low	Medium	Good	100%	Good
SHEER	[5]	Symmetric key cryptography	Hierarchical key management and authentication scheme	Authentication is achieved via HIKES	Medium	Low	Good	Good	100%	Good
SLEACH	[6]	Symmetric key cryptography		MAC	High	Medium	Medium	Limited	Probabilistic	Medium
Sec-LEACH	[7]	Symmetric key cryptography	Random key pre-distribution scheme	Don't provide broadcasts authentication	High	Medium	Medium	Limited	Probabilistic	Medium
SS-LEACH	[8]	Symmetric key cryptography	Keys pre-distribution strategy		Medium	Low	Medium	Limited	100%	Good
NSKM	[9]		Key management schemes based	MAC	Low	Low	Good	Good	100%	Good
AKM	[25]		Random Pre-distribution Key Management	Via Key Management and MAC	High	Medium	Good	Good	Probabilistic	Medium
SRPSN	[14]	Symmetric key cryptography	Group key management scheme	MAC	Medium	Low	Medium	Low	100%	Good
SecRout	[15]	Symmetric key cryptography	The Scheme introduced in LEAP [15]	MAC	Low	Low	Good	Limited	100%	Good
IKDM	[11]	Symmetric key cryptography	Bivariate polynomial-key pre-distribution mechanism	Via polynomial key pre-distribution mechanism	Low	Low	Good	Good	100%	Good
LEKM	[16]	Symmetric key cryptography	Group Key Management for Hierarchical WSNs	Identity based symmetric keys	Low	Low	Good	Limited	100%	Good
EGKMST	Our Scheme	Symmetric key cryptography	Key Management for Cluster based WSNs	Key Management & MAC	Low	Low	Good	Good	100%	Good

Table III. Security REQUIREMENTS AND Routing Attacks in WSNs.

Protocol Name	*Ref*	*Authenticity*	*confidentiality*	*Integrity*	*Freshness*	*Selective Forwarding*	*Sinkhole*	*Wormhole*	*Sybil*	*Hello Flood*	*Node Capture*
RLEACH	[3]	✓		✓		✓	+		✓	✓	
EECBKM	[4]	✓	✓	✓	✓		+		✓	✓	✓
SHEER	[5]	✓	✓	✓	✓	✓	+		✓	✓	
SLEACH	[6]	✓		✓		✓	+			✓	
Sec-LEACH	[7]	✓	✓	✓	✓	✓			✓	✓	
SSLEACH	[8]	✓	✓			✓			✓	✓	+
NSKM	[9]	✓	✓	✓	✓	✓	+	+	✓	✓	✓
AKM	[25]	✓	✓	✓	✓	✓	✓	+	✓	✓	✓
SRPSN	[14]	✓	✓	✓		✓					
SecRout	[15]	✓		✓		✓	+		+		✓
IKDM	[11]	✓	✓	✓	✓	✓	+	+	✓	✓	✓
LEKM	[16]	✓	✓	✓	✓	✓			✓	✓	+
EGKMST	Our Scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

✓ *means the protocol provides the security requirement or defeats the attack*

\+ means the protocol mitigates the effect of attack based on our pre-evaluation

Also, if we expect that the attacker requires a fixed amount of time to compromise the node, in EGKMST the keys would have changed to a new one before the attacker could use the compromised keys. Further, since the pairwise keys shared between SN and CH are different, each SN shares a unique pairwise key with its

CH. Therefore, any compromised nodes won't affect the secure communication between other sensor nodes and CH. Otherwise even if compromised node sends data using the previous key, the all data will be rejected. Thus, whole process ensures that malicious nodes won't be authenticated by the BS and also CH for intra-cluster communication. In conclusion, sinkhole and wormhole fail against EGKMST.

Theorem 4: EGKMST scheme is secure against Sybil attack.

Proof: In this attack, the attacker presents multiple identities on one node in the network [32]. In this way, the attacker mostly affects the routing mechanism. In

EGKMST scheme, the BS and nodes check the id which is attached to the message, to know the origination of the message for further action. Further, if a node tries to launch Sybil attack, it is detected during the key establishment phase. Therefore the Sybil attack fails against EGKMST.

Theorem 5: SKM may mitigate the effect of the selective forwarding attack.

Proof: In this attack an adversary only selectively forwards some messages and drops others, therefore may compromise a node [32]. In our scheme, if a cluster head is compromised, BS informs its cluster members and other CHs. Therefore, the cluster member of the compromised CH are distributed among other uncompromised CHs. Afterward BS initiates the key update mechanism, however nodes discards its currents keys and uses a new keys for future communication.

Theorem 6: EGKMST scheme can resist to hello flood attack.

Proof: In this attack, strong hello message broadcasted by attacker with high transmission power is to be received by every node in the network [32]. Other nodes

may think this message is nearest to them and sends packets by this node.

EGKMST allows every entity in the network to be confirmed or authenticated continuously. Further, if a malicious node sends data using the previous key, BS or nodes will reject all data that have received from the malicious nodes. The whole process ensures that malicious nodes will not be authenticated by nodes or the BS. In conclusion, hello flood attack can be mitigated in EGKMST scheme.

C. Comparing the performance of EGKMST with some other schemes:

In this section our EGKMST scheme is compared with some key pre-distribution schemes based on clustering structure and deterministic approach such as IKDM (an improved key distribution mechanism) and LEKM (low-energy key management protocol).

Further, in IKDM [11] as well in LEKM [16], sensor nodes communicate only with CH within the cluster. Therefore comparing in term of storage requirement of sensor node (cluster member), the key storage of EGKMST is (3 keys for SN) × key size. The key storage of IKDM can be noted as (2 keys for SN) × key size and the key storage of LEKM as (2 keys for SN) × key size. Assuming size of every key as 128 bits. Thus key storage in ordinary sensor node is: 3×128 bits for the proposed scheme, 2×128 bits for IKDM and LEKM. Therefore EGKMST as well IKDM and LEKM based on deterministic approach have lower key storage and lower communication overhead than scheme based on the random key pre-distribution, where the storage is m keys × key size. But also in the case of the node compromise, these schemes present some weakness. One drawback of LEKM is that all the keys stored in sensor nodes within a cluster are compromised, once the cluster head is captured. IKDM scheme also considers fixed cluster heads, thus one weakness of this approach is once a cluster head is captured, all the keys stored in sensor nodes in that cluster will be compromised. Therefore, it is required either to replace the sensor nodes in a cluster or replace the compromised cluster head in the cluster.

In EGKMST, it is difficult for adversary to compute the cluster group key. EGKMST also allows every entity in the network to be confirmed or authenticated continuously. Therefore, the keys are sending to only legitimate nodes. This procedure allows to reduce the chances of node compromise.

Furthermore EGKMST satisfies general security requirements, such as confidentiality by encryption using the threshold key management mechanisms and the symmetric key cryptography schemes message integrity with MAC, node authentication as mentioned before, message freshness of messages exchanged in the network with nonce and full confidentiality.

Security mechanisms, resilience against attacks and Performance requirements Comparison of EGKMST and some schemes based on probabilistic and deterministic approach are presented in Table 2 and Table 3.

VI. Conclusions And Future Work

In this paper, we propose An Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks (EGKMST). Based on hierarchical cluster structure of sensor network, the proposed scheme adopted the pair-wise key management and group key management based on threshold key cryptography to generate and to distribute the keys efficiently within a cluster and updates periodically keys. By this way, EGKMST scheme provides continuous transmission security and avoids dangerous attacks from malicious nodes and mitigate the node compromise attack in WSNs communication.

Therefore we find that the communication overhead which EGKMST protocol leads is negligible for keys establishment with low memory overhead and energy savings. The proposed scheme provides better connectivity and scalability with few messages than previous schemes based on deterministic approach and schemes based on random key pre-distribution schemes based on key pools which generate a lot of message with high storage overhead. Security and performance analysis have shown that EGKMST approach can not only provide energy savings that increase the network lifetime, but also can achieves efficient security with low key storage overhead.

Our future works may concentrate to develop and implement in the real environment a complete security protocol with low storage and energy savings.

Ackonwledgment

The work reported in this paper was supported by National Natural Science Foundation of China (No.61172049, 61003251), National High Technology Research and Development Program of China (Grant No.2011AA040101-3), Doctoral Fund of Ministry of Education of China (No. 20100006110015).

References

[1] J. Zhang, V. Varadharajan, "Wireless sensor network key management survey and taxonomy," Journal of Network and Computer Applications, vol. 33, no. 2, 2010, pp. 63-75.

[2] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for WSNs," in Proc. of the 33rd Hawaii International Conference on System Sciences, 2000, Washington.

[3] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," In Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), 2008, pp. 1-5.

[4] T. Lalitha and R. Umarani, "Energy efficient Cluster Based Key Management Technique for Wireless Sensor Network," International Journal of Advances in Engineering & Technology (IJAET), Vol. 3 No. 1, 2012, pp. 186-190.

[5] J. Ibriq and I. Mahgoub, "A secure hierarchical routing protocol for wireless sensor networks," In: Proc. 10th IEEE International Conference on Communication Systems, 2006, pp. 1-6.

[6] L. B. Oliveira, A. Ferreira, M. A. Vilaca, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "Secleach-on the security of clustered sensor networks," Signal Processing, Vol. 87, No. 12, 2007, pp. 2882-2895.

[7] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks," In Proc. 4th IEEE International Conference on Networking (ICNŠ05), 2005, pp. 449-458.

[8] D. Wu, G. Hu, and G. Ni, "Research and improve on secure routing protocols in wireless sensor networks," in 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), 2008, pp. 853-856.

[9] I. S. Gawdan, C. O. Chow, T. A. Zia, Q. I. Sarhan, "A Novel Secure Key Management for Hierarchical Wireless Sensor Networks," in Proceeding of 2011 Third Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), 2011 , pp. 312 - 316.

[10] A Diop, Y. Qi, Q. Wang, S. Hussain,"An Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks", in International Journal of Computer Science Issues (IJCSI), Jan2013. Vol. 10 Issue 1: pp 490.

[11] Y. Cheng and D. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," Ad Hoc Networks (Elsevier), vol. 5, no. 1, 2007 pp. 35-48.

[12] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, 1979, pp. 612-613.

[13] A.Chadha, Y.Liu, and S.Das, "Group key distribution via local collaboration in wireless sensor netwroks," in Proc. IEEE Sensor and Ad Hoc communications and Networks, 2005, pp. 46-54.

[14] M. Tubaishat, J. Yin, B. Panja, and S. Madria, "A secure hierarchical model for sensor network," ACM SIGMOD Record, Vol. 33, No. 1, 2004, pp. 7-13.

[15] J. Yin and S. Madria, "SecRout: A Secure Routing Protocol for Sensor Network," in IEEE 20th International Conference on Advanced information networking and applications, Vol. 1, 2006.

[16] G. Jolly, M.C. Kuscu, P. Kokate, M. Yuonis, "A low-energy management protocol for wireless sensor networks", in: Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), Kemer Antalya, Turkey, June 30-July 3, 2003.

[17] A Diop, Y. Qi, Q. Wang "An Improved Key Management Scheme for Hierarchical Wireless Sensors Networks," in TELKOMNIKA Indonesian Journal of Electrical Engineering Science, vol. 12, 2014, pp 3969-3978.

[18] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," in Proc. of the 9th ACM conference on Computer and communications security, New York, 2002, pp. 41-47.

[19] H. Chan, A. Perrig and D. Song, "Random key pre-distribution schemes for sensor networks," in Proc. of the 2003 IEEE Symposium on Security and Privacy, Washington, 2003, pp. 197-213.

[20] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in Proceedings of the 10th ACM conference on Computer and communications security, New York, 2003, pp. 62-72.

[21] Y. Zhang, Y Shen and S. Lee, "A Cluster-Based Group Key Management Scheme for Wireless Sensor Networks" In: Proc. 12th IEEE International Asia-Pacific Web Conference, 2010.

[22] P. Banerjee, D. Jacobson and S. N. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc. 6th IEEE Intl. Symposium on Network Computing and Applications, 2007, pp.145-152.

[23] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," in Proc. of the 10th Annual Network and Distributed System Security Symposium, California, 2003.

[24] P. K. Sahoo, J. J. Chen, P.i Sun. "Efficient security mechanisms for the distributed wireless sensor networks". Proceedings of the IEEE Third International Conference on Information Technology and Applications (ICITA'05). (2): 2005, 541-546.

[25] F. Kausar, A. Masood and S. Hussain, "An Authenticated Key Management Scheme for Hierarchical Wireless Sensor Networks," in Advances in Communication Systems and Electrical Engineering, Lecture Notes in Electrical Engineering, Vol. 4, 2008, pp. 85-98.

[26] H Bawa, P. Singh, R. Kumar "An Authenticated Key Management Scheme for Enhancing User Authentication in A WSN" in I. J. Computer Network and Information Security, Vol. 5(1), 2013, pp. 56-64.

[27] I S. Abuhaiba and H B. Hubboub" Reinforcement Swap Attack against Directed in Wireless Sensor Networks" in I. J. Computer Network and Information Security, Vol. 5(3), 2013, pp. 13-24.

[28] A. Modirkhazeni, N. Ithnin and O. Ibrahim, "Empirical Study on Secure Routing Protocols in Wireless Sensor Networks" International Journal of Advancements in Computing Technology, vol. 2(5), pp. 25-41, 2010.

[29] M A. Simplicio, P M. Barreto, C B. Margi, T B. Carvalho, "A survey on key management mechanisms for distributed Wireless Sensor Networks" Journal of Computer Networks, vol. 54 , pp 2591-2612, 2010.

[30] J. Zhang, V. Varadharajan, "Group-based Wireless Sensor Network Security Scheme, " In The fourth international conference on wireless and mobile communications (ICWMC 2008), 2008.

[31] A. Diop, Y. Qi, Q. Wang, "A Novel Key Management Scheme for Cluster Based Wireless Sensors Networks", In Advanced Materials Research, vol.846-847, 2014, pp. 864-847.

[32] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications, 2003, pp. 113-127.

[33] Y. Zhang, C. Wu, J. Cao and X. Li "A Secret Sharing-Based Key Management in Hierarchical Wireless Sensor Network", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, vol. 2013, pp. 1-7.

[34] Y. Y. Zhang, X. Z. Li, J. M. Liu, J. C. Yang, and B. J. Cui, "A secure hierarchical key management scheme in wireless sensor network," The International Journal of Distributed Sensor Networks, vol. 2012,Article ID 547471, 8 pp, 2012.

[35] Harn L, Lin C," Authenticated group key transfer protocol based on secret sharing", In Proceedings IEEE Trans. Comput, 2010, vol. 59 (6), pp, 842–846.

[36] D. Xu, J. Huang, J. Dwoskin, M. Chiang, and R. B. Lee, "Re-examining probabilistic versus deterministic key management," in IEEE ISIT, June 2007, pp. 2586-2590M. [Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989].

Abdoulaye Diop is presently a Ph. D candidate in School of Computer and Communication Engineering in University of Science and Technology Beijing.
His main research interests include wireless sensor networks and Network Security.

Yue Qi, received her Ph.D. degree from University of Science and Technology Beijing, China. She is a Lecturer in School of Computer and Communication Engineering in University of Science and Technology Beijing. Her research interests include computer architecture and wireless sensor networks.

Qin Wang, received her Ph.D. degree from University of Science and Technology Beijing, China. She is a Professor in School of Computer and Communication Engineering, University of Science and Technology Beijing. Her research interests include computer architecture, Very Large Scale Integration (VLSI) design and wireless sensor network.

How to cite this paper: Abdoulaye Diop, Yue Qi, Qin Wang,"Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks", IJCNIS, vol.6, no.8, pp.9-18, 2014. DOI: 10.5815/ijcnis.2014.08.02

