I. J. Computer Network and Information Security, **2015, 9, 54-63**
Published Online August 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.09.07

A Cluster based Key Management Scheme for Underwater Wireless Sensor Networks

Seema Verma
Department of Electronics, Banasthali University, Tonk, 304022, India
Email: seemaverma3@gmail.com

Prachi
Department of CSE & IT, ITM University, Gurgaon, 122017, India
Email: prachiah1985@gmail.com

Abstract—Underwater Wireless Sensor Networks (UWSNs) explore aquatic environment to facilitate various underwater surveillance applications. However, UWSN unique features also impose new challenges such as limited bandwidth, huge propagation delay, mobile nature of nodes and high error rates. UWSNs deployment in unattended environment further exacerbates their vulnerabilities to the attacks. These challenges make security solutions proposed for Wireless Sensor Network (WSN) impractical to be applicable for UWSN. This paper analyzes the problem of security and mobility in UWSN and proposes Cluster based Key management Protocol (CKP), a new key management protocol for hierarchical networks where sensor nodes form cluster around more capable nodes. CKP also proposes a new communication architecture that handles mobility efficiently and minimizes the impact of a node compromisation to itself. CKP provides confidentiality, authentication, integrity and freshness. The performance evaluation demonstrates that the CKP is energy and storage-efficient. Further, we investigate the survivability and the security of the CKP against various security threats in order to evaluate its effectiveness.

Index Terms—Cluster, Key management, Security, Mobility, Wireless sensor networks, Underwater.

I. Introduction

WSNs explore aqueous environment for resource discovery, aquatic life exploration, disaster prevention and enemy tracking. Further, they can serve as a revolutionary tool for various environment surveillance applications. Automation of Water Quality Surveillance (WQS) is one of the most significant contributions of UWSN because water is the basic requirement for human well being. UWSN significantly enhances the quality of monitoring methods and facilitates continuous and in-situ surveillance. Implementation of sensors for maintaining water quality can bring revolutionary changes in socio-economic development of society. Inspiration behind this work came from the above mentioned area of interest.

UWSN offers several benefits but at the same time they also impose challenges in terms of security because some applications like water quality surveillance, e-healthcare, etc take decision on the basis of gathered information. An adversary can insert bogus data in network so it is necessary to guarantee trustworthiness of data that is used during decision making. Consequently, robustness of UWSN against attacks and interruptions is the key for deployment of UWSN in real file applications. A number of security solutions have been presented in literature for terrestrial WSN but unique underwater characteristics such as limited battery, high error rates, dynamic topology and large propagation delay impulse us to think beyond presently available security solutions. Location of underwater nodes restricts charging of nodes by solar energy once deployed due to absence of sunlight in water. Communication via acoustic waves (lesser attenuation and larger coverage make them ideal for underwater communication) impose new difficulties in terms of short frequencies, limited bandwidth, low transmission rate, high propagation delay and energy consuming acoustic operations. Whilst ensuring resiliency, an efficient security solution should also take into consideration sensors limited battery power and mobile nature in an underwater environment. Asymmetric cryptosystem uses high energy so it became necessary to propose a lightweight symmetric security solution that is robust against attacks. In the lieu of this, we propose an efficient and resilient key management scheme based on clustering architecture that investigates the problem of security in mobile environment of UWSN and automatically adjust with topological changes. Rest of this paper is organized as follows: Section 2 discusses the related work. Section 3 includes communication architecture, mobility and attacker model. Section 4 presents description of the CKP protocol. Analysis of the performance and security of the CKP is in section 5 and the paper is concluded in section 6.

II. Related Work

A comprehensive survey of underwater characteristics, vulnerabilities, attacks and possible countermeasures is presented in [1]. Different security threats are classified in various categories [2] according to level of harm they can cause. Weakness of UWSN and their security aspects

are investigated in [3-4].

Considering the importance of security, several key management protocols are proposed in literature. Probabilistic key distribution protocols [5-8] lessen the storage and communication burden upto a certain extent but it is still high for sensor networks. EG scheme [5] is the first probabilistic protocol proposed in literature.

Authors in [9] claim that cluster based approaches optimize network bandwidth and service discovery whilst addressing scalability. LEAP, a dynamic key management protocol [10] that uses multiple keys to secure communication. LEAP uses global key for addition of new node in later stages so adversary can easily capture the node to extract global key. Moreover, LEAP assumes that sensor nodes are static in nature. SPINS [11] offer confidentiality and authentication. However, it uses the BS for establishment of pair-wise keys so limits scalability. Further, it is not immune to the Sybil attack. Asymmetric key pre-distribution scheme (AP scheme) for heterogeneous network based on clustering is designed in [12]. AP scheme is based on EG scheme. Powerful H-sensors contain more keys than other nodes of the network. This scheme has low storage but suffers from traffic analysis attack. Additionally, communication between non-compromised nodes is revealed if they share a key with compromised nodes. Moreover, AP doesn't assure optimal network coverage.

Security solutions for unique requirements of UWSNs are also presented in literature. To increase packet error rate, a multiple-path Forward Error Correction (M-FEC) scheme based on Hamming Codes is presented in [13] for underwater sensor networks. Usage of multiple paths in this scheme enhances communication and hence energy consumption. A security suite for UWSN comprising of mobile and fixed nodes was presented in [14] based on acoustic communication model to address confidentiality and integrity. However, O(n) storage overhead with n nodes network and large size message transmission. A key generation scheme using channel characteristics was presented in [15]. A new key is generated whenever there is some change in the environment. This method involves discrepancies due to long propagation delay and variation in characteristics of channel.

An underwater jamming detection protocol (UWJDP) that detects and mitigates jamming in underwater was presented in [16]. Authors in [17] described an earlier presented identity-based key agreement protocol, SOK (Sakai, Ohgishi and Kasahara). For comparison purposes, elliptic curve version of the Menezes-Qu-Vanstone authenticated key exchange protocol (ECMQV), is described. Communication overhead in ECMQV is dominated by exchange of public keys, certificates and ephemeral keys but SOK only exchange communicating party's ids. However, SOK suffers from high energy dissipation (125mJ) during pairing computation.

III. Network Model

Before we present our key management protocol it is necessary to describe network scenario, mobility and attacker model for which we design our protocol.

A. Communication Architecture

A WSN typically comprises of resource constrained sensor nodes and the Base Station (BS). Several organizations of WSN have been proposed in literature for different communication patterns (direct, multi-hop, static and dynamic clustering) and security solutions designed for one architecture might not go well with another. So, prior to presenting any security solution it is necessary to discuss the communication architecture for which we designed this security solution.

In proposed architecture, sensor nodes form dynamic clusters around highly capable nodes (Cluster Head) because recent researches [18-20] claim that heterogeneous networks are more energy efficient, scalable and have higher network lifetime than homogeneous. We use cluster based architecture because it minimizes topological changes, propagation delay and enhances network lifetime by effectively utilizing network bandwidth [21]. The proposed network scenario also comprises a Base Station (BS) that collects data directly from CHs and forwards it to outside world. It is a laptop type device that possesses sufficient battery life and enormous memory to store node ids and their cryptographic primitives. BS is also equipped with acoustic transceiver (to communicate with sensors) and radio transceiver (to communicate with outside world). CHs possess higher range acoustic modem (UWM4000) to broadcast or transmit information directly (gathered from its members) to BS. They perform majority of computation and communication operations because energy dissipation is not a major issue for them. Sensor nodes are deployed with short range acoustic modem (UWM2000) and whenever they want to transmit something they directly send it to their CHs i.e. communication between sensors and their CHs is one-hop. As a result, compromisation of a node doesn't affect other nodes in any manner. Furthermore, nodes in shallow water have high mobility rates due to various sea surface activities when compared to nodes in deep water. So, in order to minimize network reaction to topological changes, utilize energy resources efficiently, increase network lifetime and provide optimal coverage we deploy fixed and powerful CHs in shallow water at pre-defined locations. Mobile nodes are deployed in shallow as well as in deep water. We have chosen this deployment scenario because water current drifts CHs much quickly and movement of CH makes that cluster useless until nodes of that cluster moves in territory of another CH. Within each cluster, a CH maintains secure communication among the cluster members and itself.

B. Mobility Model

Our mobility model takes into account fluid nature of medium because sensors are driven by water current and dispersion. For mobility pattern, we use random waypoint mobility model. Cluster nodes move randomly in different directions with minimum, medium or maximum pre-defined speed. Minimum speed is 1meter/second,

medium speed is 3meter/second and maximum speed is 5 meter/second. Mobile nodes are deployed with Autonomous Underwater Vehicles (AUVs) and they regulate their depth and position collaboratively to provide optimal coverage. CHs are deployed at fixed pre-defined locations to provide optimal coverage of network. CHs are fixed with buoy to minimize mobility and membership events. Edges are time dependent because existence of links varies continuously according to changing channel characteristics and mobility model.

C. Attacker Model

Deployment in unattended/hostile environment and broadcast nature of the wireless communication make UWSN susceptible to numerous security threats. Intruders can easily intercept communication, overhear plain messages or capture sensor nodes to retrieve information stored on them. UWSN are more susceptible to underwater attacks because they are exposed to node mobility, external noise and frequent environmental changes. This paper aims to detect and handle all internal threats imposed by the attacker. Comprising a node means an attacker can retrieve all the information stored on a node. Nodes don't trust each other so they directly send their readings to CH. An adversary can attack network in different scenarios. An adversary may capture a node and extract sensitive information stored on it. Thereafter, he may alter it in order to generate forged information for end user. In an another scenario, even if we assume that sensitive information is encrypted, an adversary can still alter the information without understanding its actual meaning to render it useless. An adversary may also inject some nodes in network in order to insert wrong information or capture sensitive information. In addition, an adversary can replicate (masquerade) id of an existing authentic sensor to capture susceptible information of network. Additionally, by capturing some nodes of cluster adversary may attempt to launch collusion attack and gain access over entire cluster. This phenomenon is known as collusion attack. Attacker may also try to exhaust battery of sensors by repeatedly sending same information in the network. An adversary can also launch attacks like selective forwarding, HELLO flood, Sybil, wormhole and sinkhole.

IV. Cluster based Key management Protocol

CKP is a key management protocol that offers confidentiality, integrity, authentication, freshness and collusion attack. Additionally, it satisfies various performance and security requirements.

A. Assumptions

We made the following assumptions about the key management protocol we are using:

BS communicates with outside world so compromisation of the BS leave entire network useless. Therefore, we assume that the BS is immune to any kind of attacks.

CHs carry entire information about clusters so they are more prone to attacks. Deploying them with tamper resistant material don't increase much cost because they comprise very small portion of the network.

Sensor nodes are not equipped with tamper resistant material due to cost constraints.

Sensor nodes don't trust each other.

B. Overview

Security protocols require different level of security at different stages. Consequently, a single key mechanism is not sufficient for all types of secure transmission in UWSN. CKP supports keys for different purposes. Here, we discuss those keys in detail:

- Network Key: All nodes of network share this key. It is used to encrypt messages that BS broadcasts to all the nodes of network. For security concerns, this key must be erased from nodes prior to minimum time required to capture a node and extract some information from it.
- Group Key: This key is shared among CH and its members. It is used to secure multicast messages that CH sends to its members. Nodes use this key to encrypt message that doesn't carry highly sensitive information for e.g. join request messages.
- Pair-wise Key: BS pre-loads every sensor with an unique pair-wise key. Later on, BS sends these keys of sensors to their respective CH. Every sensor encrypts sensitive readings/information with its pair-wise key and sends it to the CH. This phenomenon doesn't allow a compromised node to retrieve any information from other nodes and limits the impact of a node capture to itself.

C. Notations

In this paper, the following notations are used to explain CKP and its cryptographic operations:

Nonce is a random string used to achieve freshness.

CH_i /S_i denotes the ith Cluster Head/Sensor.

id_{CHi}/id_{Si} denotes the id of ith Cluster Head/Sensor.

MAC_k(Msg) is Message Authentication Code of message Msg with the encryption key k.

E_k(Msg) is the encryption of message Msg with the encryption key k.

$idlist_{sensors}$/$idlist_{authentic\_sensors}$ denotes a list that comprises of ids of sensors/authentic sensors.

$list_{pairwise\_keys}$ denotes a list of pair-wise keys corresponding to authentic sensors.

c_i denotes counter initialized to some random value by BS for ith CH.

x_i denotes counter initialized to some random value by ith CH for its members.

$slot_{si}$ denotes time slot assigned to ith sensor.

D. Protocol Description

In this section, we give the detailed description about establishment of secure communication inside and outside a cluster using CKP.

- Key generation and distribution phase: BS generates

global key, n unique node ids, n pair-wise keys and n/10 group keys where n is the number of nodes in network. Further, it pre-loads every node with an unique id, a global key and a pair-wise key. Additionally, it assigns every CH an unique group key.

- Cluster setup phase: Every CH periodically broadcasts a message encrypted with global key (because energy is not a major issue for CHs) that comprises of CH's id, group key, nonce (for freshness) and MAC generated with the help of global key (used for the purpose of authentication and integrity).

$$CH_i \rightarrow *: \begin{pmatrix} id_{CHi}, E_{global\_key}(group\_key, nonce), \\ MAC_{global\_key}(group\_key \mid id_{CHi}) \end{pmatrix}$$

All nodes decrypt messages sent by CHs to retrieve group keys and immediately delete their global key. Afterwards, nodes select their nearest CH based on received strength of signals and send a join request message encrypted with group key to the chosen CH.

$$S_i \rightarrow CH_i : (E_{group\_key}(id_{si}), MAC_{group\_key}(nonce \mid id_{si}))$$

Nodes ids are sent during join request message, nodes send their ids in encrypted form to prevent authentic sensors ids from snooping. Otherwise, an attacker can insert a new sensor in network and masquerade it with authentic sensor id. Moreover, to ensure freshness as well as reduce size of message (for energy efficiency), sensor incorporates the earlier sent nonce in MAC (not send in message). Now, CHs form a list containing ids of sensors that sent request message and send it to BS in encrypted form.

$$CH_i \rightarrow BS : \begin{pmatrix} id_{CHi}, E_{k_{CHi}}(idlist_{sensors}), MAC_{k_{CHi}}(id_{CHi} \mid \\ number\_of\_sensors\_in\_idlist_{sensors}) \end{pmatrix}$$

If BS finds some malicious sensor ids then delete them from idlistsensors. BS sends list of n authentic sensor ids (n<=m) along-with their preloaded keys, a counter (ci is a random value that is unique for every CH) and MAC to the CH. Counter ci is used to guarantee freshness of messages among the CH and the BS and its value is incremented by one each time the CH sends a packet to the BS.

$$BS \rightarrow CH_i : \begin{pmatrix} E_{k_{CHi}}\left(idlist_{authentic\_sensors}, list_{pairwise\_keys}, c_i\right), \\ MAC_{k_{CHi}}\begin{pmatrix} number\_of\_sensors\_in \\ \_idlist_{authentic\_sensors} \end{pmatrix} \end{pmatrix}$$

CH multicasts a join response message to its authentic sensors that comprises of sensor ids, their schedule and xi (avoid replay attack among sensors and their CH). x_i is a random value generated by the CH. This message comprises of various sub-messages. Each sub-message is encrypted with a separate pair-wise key. CH assign slots and members of a cluster send data in assigned slot to avoid collision and minimize communication/energy consumption.

$$CH_i \rightarrow *: \left(E_{k_{S1}} < id_{s1}, slot_{s1} >, ..., E_{k_{sn}} < id_{sn}, slot_{sn} >\right),$$
$$E_{group\_key}(x_i), MAC_{group\_key}(id_{CHi} \mid x_i)$$

- Data gathering phase: Since we are working on water quality surveillance applications and nodes in proximity measure similar values so instead of sending redundant value in limited bandwidth UWSN nodes remain in sleep state for most of the period and wakes up at specified intervals to gather information and sends to CH turn-wise using TDMA. This low duty cycle operation consumes very less energy and enhances network lifetime considerably.

$$S_i \rightarrow CH_i : \left(id_{CHi}, E_{k_{si}}(data), MAC_{k_{si}}(id_{si} \mid id_{CHi} \mid x_i + a)\right)$$

Initially, a is 0 and its value is incremented each time a sensor sends a message to the CH.

- Data forwarding phase: Upon receiving data from its members, CH performs selective forwarding. They determine whether the received value is in standard range or not. If received value is not in standard range then CH waits for response of two more members. If all of them send values deviated from standard range then it processes and aggregates their values to retrieve meaningful information and immediately forwards it to BS.

$$CH_i \rightarrow BS : \begin{pmatrix} id_{CHi}, E_{k_{CHi}}(aggregated\_data), \\ MAC_{k_{CHi}}(id_{CHi} \mid c_i + b) \end{pmatrix}$$

Similar to a, b is initialized with 0 and incremented each time CH sends a message to the BS. If received value is in standard range the CHs don't forward any data. This method effectively utilizes UWSN's limited resources and enhances the network lifetime

E. Membership Events

- Node Addition: During the entire tenure of WSN it may be necessary to add some new nodes in the network. Here, we present the way of adding new nodes in the existing network. New nodes are deployed randomly in network and unaware of their CHs. BS pre-loads the new node with a pair-wise key. New node determines its nearest CH based on periodic broadcasts from CHs and sends a join

request message to its nearest CH encrypted with its pair-wise key.

$$S_i \rightarrow CH_i : (E_{k_{si}}(id_{si}), MAC_{k_{si}}(nonce \mid id_{si}))$$

Corresponding CH forwards it to BS.

$$CH_i \rightarrow BS : \left(id_{CHi}, E_{k_{si}}\left(id_{si}\right), MAC_{k_{CHi}}\left(id_{CHi} \mid E_{k_{si}}\left(id_{si}\right)\right)\right)$$

If authentic, BS sends pair-wise key of new node and a new counter to CH.

$$BS \rightarrow CH_i : \begin{pmatrix} E_{k_{CHi}}\left(id_{si}, pairwise\_key_{si}, c_i\right), MAC_{k_{CHi}} \\ \left(id_{si} \mid pairwise\_key_{si}\right) \end{pmatrix}$$

Now, CH decrypts id of transient node from previously sent message and sends a message that comprises of new time schedule and xi value.

$$CH_i \rightarrow *: \begin{pmatrix} E_{k_{S1}} < id_{s1}, slot_{s1} >, ..., E_{k_{si}} < id_{si}, slot_{si}, \\ group\_key >, .., E_{k_{sn}} < id_{sn}, slot_{sn} > \end{pmatrix},$$
$$E_{group\_key}\left(x_i\right), MAC_{group\_key}\left(id_{CHi} \mid x_i\right)$$

This message also serves as join acknowledgement for recently joined sensor. Now, new node can securely transmit data to its elected CH.

- Node Removal: Whenever a node is removed due to malicious behavior or exhaustive battery CH delete its id and pair-wise key and notifies the BS about the same. BS either deletes node's id from its database or assigns it to new nodes.
- Node Transition: Whenever a node makes transition from one cluster to another due to weak signal strength it notifies its current CH about its departure. Current CH deletes node's id and pair-wise key from its database and forwards its departure information to the BS. Departing node transmits a join message to its nearest CH in a way similar to node addition.

V. Performance Evaluation Of CKP

In this section, we evaluate and performance of CKP based on various parameters.

A. Energy Consumption

Energy required in transmitting 1Kb of information over a distance of 100 meters is same as energy used by 100MIPS/W power processor to effectively execute 3 million instructions[22]. This fact is more evident in case of acoustic communications. Moreover, energy consumption during cryptographic operations differs from one hardware to another. Thus, in CKP we determine energy consumption involved during communication and not during cryptographic operations.

Table 1. Ckp Energy Consumption During Communication

Phase	Member	Transmission (Joule)	Reception (Joule)	Total (Joule)
Cluster formation	CH	3.71	0.46	4.17
	Member	0.12	0.14	0.26
Data gathering				
	CH	NA	0.17	0.17
Data forwarding	Member	0.42	NA	0.42
	CH	1.51	NA	1.51
	Member	NA	NA	NA
Node addition	CH	2.71	0.13	2.30
	Member	0.12	0.15	0.27
Node removal				
	CH	2.71	0.17	2.34
Node transition	Member	0.24	0.09	0.33
	CH	0.49	NA	0.49
	Member	NA	NA	NA

We use acoustic communication model to calculate energy dissipation. It consumes 416.66 μJ and 1458.33 μJ energy for transmission and 83.33 μJ and 166.66 μJ energy for reception over 1200m and 4000m respectively [23]. We make the following assumptions about sizes:

All node Ids, counters and time slots are 32 bits in length.

All keys, MACs, nonce are 128 bits.

The sensed, gathered and processed information is 500 bits.

Table 1 demonstrates the energy consumption by a node and the CH for execution of one instance of CKP (Energy dissipation of BS is excluded because it is assumed to have unlimited battery life). Here, we assume a network scenario that comprises of total 40 nodes (10% CHs and 90% cluster members) and discuss major phases of CKP that contribute to the energy dissipation.

In cluster formation phase, energy consuming

transmissions such as join acknowledgement and authentication from the BS are performed by CHs because energy dissipation is not a major concern for them. Further, energy dissipation in transmission of slots during join acknowledgement is negligible when compared to energy consumption involved with continuous sensing and sending. Data gathering phase is quite expensive for sensors however to efficiently utilize network bandwidth every sensor perform this operation once in n instances if n is the number of members in a cluster i.e. energy consumed in this operation by a sensor is inversely proportional to number of members in that cluster. Data forwarding phase involve transmission by the CH only if gathered values are out of bound. Majority of the energy intensive operations are performed by the CH during node addition and transition. It is clear from the table 1 that communication burden is majorly shifted to CHs.

B. Storage overhead

Security is an auxiliary operation for resource constrained sensor nodes. Storage requirement of a key management scheme is a deciding factor for its implementation in sensor networks. Prior to deployment, every cluster member stores an unique id, a global key and a pair-wise key. Further, every CH has an initial requirement of a unique id, a global key, a group key and a pair-wise key. This leads to an initial storage requirement of 288 bits for a cluster member and 416 bits for a CH.

After deployment, every node of network deletes its global key. Further, every cluster member stores its id, a group key corresponding to its CH, a pair-wise key and a counter. CH stores its id, a group key, t+1 pair-wise keys if it has t members (one for BS) and two counters (one for BS and another for its members). As a result, cluster member and CH require 320 bits and (224+128.(t+1)) bits storage respectively. Most commonly used sensor nodes (MicaZ Mote) support 4 KB runtime memory, 128KB program memory and 512 KB external memory [24]. So, storage overhead associated with the CKP is quite reasonable for recently available sensors in the market.

C. Security Analysis

Hierarchical architectures are more secure than non-hierarchical ones because they localize the impact of compromisation. In most of clustering protocols, compromisation in one cluster doesn't affect other cluster in any manner. However, this is not the case with most of the non-hierarchical protocols. CKP is one step ahead in terms of achieving resilience because every node shares an unique and independent key with its CH so compromisation of a node doesn't reveal anything about other nodes. In this section, we analyze the security features of proposed protocol. Initially, we discuss survivability of the CKP under undetected attacks. Later on, we evaluate its resilience to defend against various attacks.

- Survivability: Whenever a node is captured, the attacker can retrieve all sensitive information from it for e.g. its keys. If any compromised node is detected then node is revoked from the network and both the CH and the BS delete its key and id. Further, CH updates its group key and sends it to its members by encrypting it with their corresponding pair-wise keys. However, compromisation detection is not easy in UWSNs due to their deployment in unattended environment at remote locations. Thus, it became necessary to evaluate effectiveness of the CKP in terms of security for undetected attacks.

  First, by possessing node's unique id, pair-wise key and counter an adversary can inject/insert/send false information to the CH. However, in CKP instead of relying on reading of a single (malicious) sensor, CH waits for response of two more sensors. As a result, when an adversary alters information, CH easily identifies it with the help of readings of authentic sensors.

  Second, a cluster member doesn't establish any trust relationship with its neighbors in CKP. So, compromisation of a node doesn't affect its neighbors.

  Third, access to the group key allow attacker to decrypt messages multicast by the CH but multicast messages don't carry any sensitive information. They generally comprise of counter. Further, since we periodically update group key so the attacker can only decrypt the few messages that are encrypted by the current group key.

  Fourth, the global key always remains a security concern so we restricted use of global key for very short duration. To ensure security, time duration of broadcasts by CHs must be less than minimum amount of time required to retrieve information from any node by an attacker in CKP. Authors in [25] demonstrate that an adversary require atleast 10 seconds in order to capture a node and retrieve some information from it. Security remains a concern in LEAP because new nodes are added in the network with same global key and an adversary can compromise new node before completion of initialization phase. Unlike LEAP, to minimize destruction impact the CKP inserts new nodes in the network without the global key. In worst case, if global key can be compromised before the minimum time required in capturing a node then adversary can only retrieve group keys and don't disclose anything but ids of sensors that sent join request message to the CH. In a mobile environment, membership of clusters tends to change quite frequently so information about initial membership of the cluster become useless for the attacker after some time.
- Security against different attacks in CKP: An attacker may launch various attacks [26] in sensor networks such as injects false information, modifies sensitive readings and replays old packets to exhaust limited battery life of sensors. Proposed scheme is immune to these attacks because it accepts

information only from the authentic node, transmits sensitive information in encrypted form (with keys possessed by authorized users), associates MAC with every transmission to ensure integrity and authentication (because underwater wireless transmission is a very lossy transmission and MAC assures both authenticity and integrity and avoids use of other mechanisms required to check integrity such as CRC) and incorporates counters to avoid replay attack. When an attacker compromise a node and alter its sensitive information, CH can easily detect it because it doesn't take decision solely on the basis of a single node. Also, as soon as a compromised node is detected, CH immediately revokes it from the network and updates its group key. Further, attacker may induce selective forwarding where a compromised node refrains from forwarding packets of few selected nodes while reliably forwarding packets of other nodes. CKP handles this effectively because authentic nodes directly forward the gathered information to trusted CHs and they directly forward it to the BS.

CKP also prevents the HELLO flood attack. In this attack, an adversary starts broadcasting HELLO messages with high transmission power to make all nodes believe that it is nearest to them. If HELLO flood attack succeeds then all nodes will start sending join request messages to the adversary and quickly exhaust their battery. However, this attack will not succeed in CKP because every CH broadcasts messages encrypted with global key and an attacker doesn't possess global key.

A node claims to have several identities in case of Sybil attack [27, 28]. An adversary can use this attack to forge multiple fake ids and present itself as multiple nodes. Sybil attacks are major security concern for WSN. CKP provides robustness against this attack because CH verifies identities of nodes with BS.

Sinkhole [27] and Wormhole [29, 30] attacks are most difficult to identify. In sinkhole attack, node attracts traffic from other nodes of the network (by broadcasting forged data like high residual energy, high transmission power) and later drops it. In CKP, CHs broadcast join request in encrypted form and attacker doesn't possess key. Moreover, nodes only send their reading to trusted CHs so sinkhole attack will not succeed. In case of wormhole attack, adversary captures information on one end and replays it on another end of network to restrict nodes from forwarding information on routes longer than one or two hops. Wormhole attack can occur even if no node is compromised and security protocol provides confidentiality, integrity and authenticity. For wormhole attacks, it is necessary to compromise at least two sensor nodes that communicate but in CKP nodes don't communicate with their neighbors so attacker will not succeed in launching of wormhole attack. So, interaction with only trusted nodes (CHs in our case) is critical to prevent wormhole attacks. In addition, all keys are independent of each other so CKP offers forward as well as backward confidentiality.

CKP doesn't deal with Denial of Service (DoS) attack because we are operating on a wireless channel so an adversary can always put a strong signal on wireless channel to jam it for any useful transmission. Also, an attacker can repeatedly send join request messages to CH with random ids to exhaust its resources. However, this attack is not serious in CKP because CH is a resource rich node.

D. Impact of Mobility

Pre-determined locations of CHs work well for static network but location of nodes tends to change in aqueous environment due to water current. To limit mobility, avoid frequent reestablishment of cluster, enhance network throughput and lifetime, CHs in CKP are fixed with the help of wire. We investigate the impact of mobility when UWSN is deployed with static CHs and mobile cluster members. Figure 1 demonstrates average of 10 simulations for different speed of nodes. Difference in distance is evident when node mobility is high.

Distance is very crucial parameter in underwater environment and requires utmost attention because transmission distance is directly proportional to energy dissipation and propagation delay. Moreover, transmission loss also depends upon distance because transmission loss occurs either due to spreading or attenuation and both these parameters depend on distance. Furthermore, high frequencies induce huge attenuation over large distance. So, small propagation distance also enables use of high frequencies in water.

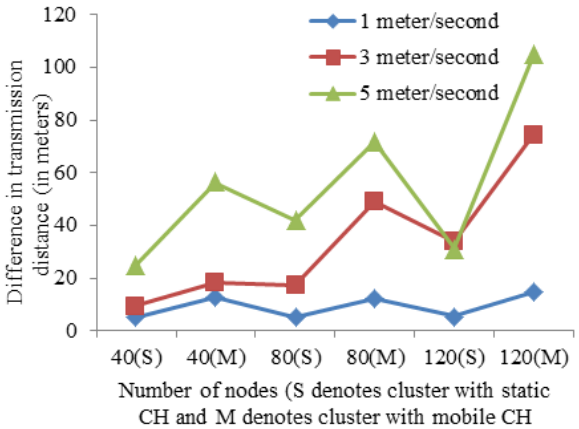

Fig.1. Difference in transmission distance over different network sizes

E. Number of CHs

Different number of CH results in uneven energy consumption. Choice of number of clusters depends on various parameters like topology of network, size of network, etc. Transmission distance between nodes and their CH and between the CH and the BS varies with the number of CHs. Small number of CH increases transmission distance within the cluster and hence energy

consumption. Large number of CHs decrease effectiveness of aggregation, increase number of transmissions from CH to BS, cost associated with powerful nodes and energy dissipation.

Figure 2 depicts variation in transmission distance with increase in CHs from 5 to 40%. It is clear from the figure that distance remains minimized when 10% of nodes are chosen as CH. So, CKP uses 10% of nodes as CH in its network scenario.

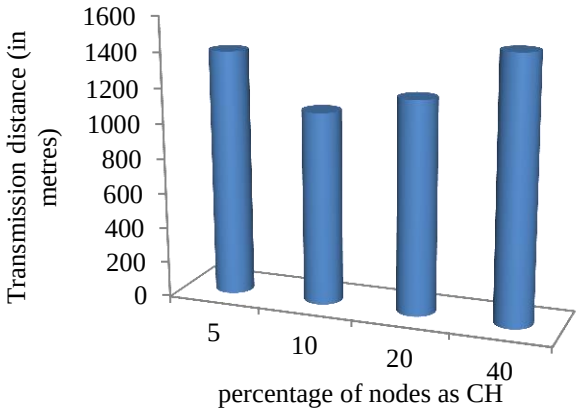

Fig.2. Difference in distance with varying number of CH

F. Comparison

Table 2 depicts key connectivity, storage overhead, energy dissipation and resilience of EG, AP, LEAP and CKP where p is the probability of sharing keys, n is the number of nodes in network, d is the average number of neighbors. P is size of key pool, k is the size of key ring in EG scheme. M denotes number of keys hold by H-sensors and l is the number of keys hold by L-sensors.

In CKP, CH holds keys for all members of the cluster and sensors in this scenario communicates directly with their CH so key connectivity offered by CKP is higher than that of EG and AP scheme. AP scheme reduces the storage burden in comparison to EG but it is still high. LEAP and CKP keep it at minimum with 1 and 2 keys respectively. Storage burden of LEAP increases in later stages but it remain same in case of CKP throughout the network lifetime. CKP restricts the impact of node compromise to itself whereas it is high in case of EG and LEAP. Note that even if global key is captured in CKP before the initial key establishment phase it cannot extract anything more than node ids but in case of LEAP it will compromise the whole network. Further, LEAP uses global key during node addition and it is easy for the adversary to capture it in a hostile environment. Unlike LEAP, global key is not used during node addition in CKP and retrieve everything from the network. In AP, impact of compromise depends upon values of M and l. CKP and LEAP prevents attacker from launching sinkhole/wormhole attack because nodes communicates with trusted nodes only. Keys in CKP are independent of each other so unlike other protocols it provides forward and backward confidentiality

Table 2. Comparison of Ckp with Other Protocols on Various Parameters

Parameters	EG	AP	LEAP	CKP
Key connectivity	$p = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}$ k	$p = 1 - \frac{(P-M)!(P-l)!}{P!(P-M-l)!}$ l	1	1
Initial key storage overhead			1	2
Compromised network due to node capture	p.(n-1)	slightly lesser than p.(n-1)	d	1
Resilience against Sinkhole/Wormhole attack	No	No	Yes	Yes
Forward confidentiality	No	No	No	Yes
Backward confidentiality	No	No	No	Yes

VI. Conclusion

We have presented a Cluster based Key management Protocol, a key management protocol for UWSN. Our scheme includes various types of keys to offer different level of security at different stages in a mobile environment. It presents a secure way of UWSN organization that handles mobility effectively with the help of heterogeneous nodes. It prevents majority of attacks or strongly restricts them upto a great extent. Further, it limits the impact of node compromise to itself by directly communicating with the Cluster Heads or Base Station. Key establishment and update procedure followed in Cluster based Key Management Protocol is energy and storage efficient since entire network is not disturbed and sensor nodes are supposed to store minimal number of keys.

References

[1] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun*., vol. 18, no. 1, pp. 22-28, 2011.

[2] Y. Dong and P. Liu, "Security considerations of underwater acoustic networks," in *Proceedings of 20th*

International Congress on Acoustics, Sydney, Australia, August 23-27, 2010.

[3] H. Jiang, Y. Xu, "Research Advances on Security Problems of Underwater Sensor Networks," *Advanced Materials Research*, vol. 317-319, pp. 1002–1006, Aug 2011.

[4] G. Yang, Z. Wei, Y. Cong, D. Jia, "Analysis of security and threat of underwater wireless sensor network topology," in *Fourth International Conference on Digital Image Processing*, Kuala Lumpur (Malaysia), Apr 7-8, 2012, vol. 8334, pp. 274-277, DOI: doi:10.1117/12.968205.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," i*n Proceedings of the 9th ACM conference on Computer and Communication Security*, New York, USA, Nov. 18, 2002, pp. 41-47, DOI: 10.1145/586110.586117.

[6] H. Chan, A. Perrig, D. Song, "Random key pre-distribution schemes for sensor networks", in *Proceedings of IEEE Symposium on Security and Privacy*, IEEE Computer Society Washington, DC, USA, May 11, 2003, pp. 197-213 , DOI:10.1109/SECPRI.2003.1199337.

[7] S. Hussain, M. Rahman, L. Yang, "Key pre-distribution scheme using keyed-hash chain and multipath key reinforcement for wireless sensor networks," IEEE Computer Society, Los Alamitos, CA, USA, Mar 9, 2009, pp. 1–6, DOI:10.1109/PERCOM.2009.4912893.

[8] V. T. Kesavan, S. Radhakrishnan, "Multiple Secret Keys based Security for Wireless Sesnor Networks," *International Journal of Communication Networks and Information Security*, vol. 4, no. 1, pp.68-76, 2012.

[9] M. Dohler, T. Watteyne, F. Valois, J. Lu, "Kumar's, Zipf's and Other Laws: How to Structure a Large-Scale Wireless Network?" *Annals of Telecommunications*, vol. 63, no. 5-6, pp. 239-251, May-June 2008.

[10] S. Zhu, S. Setia, S. jajodia, "LEAP: efficient security mechanisms for large scale distributed MSN networks," in *Proceedings of the 10th ACM conference on Computer and Communication Society*, Washington DC, Oct. 27-30, 2003, pp. 62-72, DOI: 10.1145/948109.948120.

[11] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security Protocol for Sensor Networks," in *Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rome, Italy*, July 16-21, 2001, pp. 189-199, DOI: 10.1145/381677.381696.

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

[13] Junfeng Xu, Keqiu Li and Geyong Min, "Reliable and Energy-Efficient Multipath Communications in Underwater Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 7, pp. 1326-1335, Jul 2012.

[14] Gianluca Dini and Angelica Lo Duca, "A Secure Communication Suite for Underwater Acoustic Sensor Network," *Sensors*, vol. 12, no. 11, pp. 1-27, Nov. 2012, DOI: 10.3390/s121115133

[15] Yicong Liu, Jiwu Jing and Jun Yang, "Secure Underwater Acoustic Communication Based on a Robust Key Generation Scheme," in *Proceedings of 9th international conference on Signal Processing*, Beijing, Oct. 26-29, 2008, pp. 1838-1841, DOI: 10.1109/ICOSP.2008.4697498.

[16] Sudip Misra, Suraj Dash, Manas Khatua, Athanasios V. Vasilakos and Mohammad S. Obaidat, "Jamming in underwater sensor networks: detection and mitigation," *IET Communications*, vol. 6, no. 14, pp. 2178-2188, Sep. 2012.

[17] D. Galindo, R. Roman and J. Lopez, "A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks," in *Proceedings of the 7th International Conference on Cryptology and Network Security*, Hong Kong, China, Lecture Notes in Computer Science 5339, December 2-4, 2008, pp. 120-132, DOI: 10.1007/978-3-540-89641-8_9.

[18] L. Girod, T. Stathopoulos, N. Ramanathan, J. Elson, D. Estrin, E. Osterweil and T. Schoellhammer, "A system for simulation, emulation, and deployment of heterogeneous sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, New York, USA, Nov. 3, 2004, pp. 201-213, DOI:10.1145/1031495.1031519.

[19] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar and N. Shroff, "A minimum cost heterogeneous sensor network with a lifetime constraint," *IEEE Transactions on Mobile Computing*, vol. 4, no. 1, pp. 4-15, Jan-Feb 2005.

[20] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu and S. Singh, "Exploiting heterogeneity in sensor networks," in Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, vol. 2, Mar 13-17, 2005, pp. 878-890, DOI:10.1109/INFCOM.2005.1498318.

[21] X. Du, Y. Xiao, "Energy efficient chessboard clustering and routing in heterogeneous sensor network," *International Journal of Wireless and Mobile Computing*, vol. 1, no. 2, pp. 121-130, Feb 2006.

[22] G. J. Pottie and W. J. Kaiser. "Wireless integrated network sensors," *Communications of the ACM*, vol., no., pp. 51–58, May 2000.

[23] Link Quest Underwater Acoustic Modems, http://www.link-quest.com/html/uwm_hr.pdf.

[24] Crossbow technology, http://www.xbow.com.

[25] R. Anderson and M. Khun, "Tamper resistance-A cautionary note," in *proceedings of the 2nd USENIX Workshop on Electronic Commerce*, Berkeley, CA, USA, vol. 2, Nov 18, 1996, pp. 1-11.

[26] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in *Proc. of First IEEE Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, USA, May 11, 2003, pp. 113-127, DOI: 10.1109/SNPA.2003.1203362.

[27] J. Douceur, "The Sybil Attack," in *First International Workshop on Peer-to-Peer Systems*, Verlag, London, UK, Mar 7, 2002, pp. 251-260.

[28] Xun Li ; Guangjie Han ; Aihua Qian ; Lei Shu ; Rodrigues, J., "Detecting Sybil attack based on state information in Underwater Wireless Sensor Networks," *21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Primosten, 18-20 Sept., 2013, pp. 1-5, DOI: 10.1109/SoftCOM.2013.6671865.

[29] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," in *Proceedings of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, San Francisco, CA, vol. 3, Mar 30- Apr 3, 2003, pp. 1976-1983, DOI: 10.1109/INFCOM.2003.1209219.

[30] Honglong Chen, Wendong Chen, Zhibo Wang, Zhi Wang, and Yanjun Li, "Mobile Beacon Based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2014, 2014.

Authors' Profiles

Dr. Seema Verma received her PhD at Banasthali University. She is a Reader (Associate Professor) at the Department of Electronics, Banasthali University, Rajsthan, India. Her research interests include issues related to communication System, wireless communication, VLSI Design, MIMO - of DM, cryptography & networks security, turbo codes, LDPC codes. She is author of 73 refereed articles in these areas, 30 in reputed international journal and 43 in International Conferences. She has coauthored five books. She is a Fellow of IETE and member of Indian Science Congress, ISTE.

Ms. Prachi is currently pursuing Ph.D. in Computer Science at the Banasthali University of Rajasthan, India. Her current research interests include key agreement in wireless peer-to-peer systems and security in underwater sensor networks. Prachi received the B.Tech. degree from M.D. University, Rohtak in 2007 and the M.Tech. degree in Computer Science from the Banasthali University at Rajasthan in 2009. She is currently a Ph.D. student in the Department of Computer Science at the Banasthali University, Rajasthan.

How to cite this paper: Seema Verma, Prachi,"A Cluster based Key Management Scheme for Underwater Wireless Sensor Networks", IJCNIS, vol.7, no.9, pp.54-63, 2015.DOI: 10.5815/ijcnis.2015.09.07

