수중 음향 센서 네트워크를 위한 안전한 시간 동기화 기법 연구

신승목*, 김광조*

*한국정보통신대학교, 국제정보보호기술연구소

A Study on secure time synchronization protocol for underwater acoustic sensor network

Sung-mok Shin*, Kwangjo Kim*

*International Research Center for Information Security(IRIS),

Information and Communications University (ICU)

요 약

최근에 관심이 증대되고 있는 수중 센서 네트워크에서는 라디오 주파수의 수중 감쇠현상 때문에 음향 통신을 활용하고 있다 [2, 3]. 그래서 기존 육상에서 사용하던 라디오 기반의 네트워크 프로토콜을 그대로 적용하기가 어려워 새로운 통신 프로토콜의 연구가 필요한 실정이다. 그 중에 선결되어야 할 과제가 시간 동기화이다. 센서 네트워크에서 시간 동기화 기술은 동기 기반 통신 프로토콜 개발뿐만 아니라 기록된 이벤트들의 발생순서 구분 등 다양한 응용을 위해 필수적이다 [1]. 이러한 중요성 때문에 시간 동기화에 대한 악의적인 공격이 발생할 경우, 각 센서 노드들의 시간이 일치되지 않아, 측정된 데이터의 신뢰성이 저하되고, sleep-wakeup 스케줄에 이상이 발생하는 등, 큰 문제가 발생할 수 있다 [6, 7]. 본 논문에서는 수중 센서 네트워크를 위해 제안된 시간 동기화 기법 [8, 9]들과 기존에 육상 환경에서 제안된 보안을 고려한 시간 동기화 기법 [6, 7]에 대해 살펴본다. 이를 기반으로 기존 보안 기법들의 수중 환경에의 적용 가능성과 향후 수중 센서 네트워크에서 다루어야 할 보안 사항에 대해 알아본다.

I. 서론

센서 네트워크의 기술이 발전하고 그에 따른 관심이 커짐에 따라 센서 네트워크 기술을 이용하여 인간이 접근하기 힘든 환경에서 여러 가지 필요한 정보들을 얻으려는 시도가 이루어지고 있다. 특히 수중 센서 네트워크는 강이나 깊은 바다에 설치되어 수중 탐사, 자연재해 방지, 무인 감시 시스템 등의 응용으로 이용이 가능하다. 이러한 희망적인 전망에도 불구하고 수중 센서 네트워크는 물속이라는 특수한 환경에서 동작을 하기 때문에, 네트워크 통신에 있어서 많은 제약 사항을 가진다 [2, 3]. 특히 육상 센서 네트워크에서 주로 사용되던 라디오 주파수은 물속에서 심각한 감쇠 현상으로 인해 사용이 불가능하다. 그래서 수중 센서 네트워크에서는 주로 음향통신을 이용하게 된다. 그러나 음향 통신은 약 1500m/s의 속도를 가지므로 전파 지연 시간이 길고 제한된 대역폭을 가지므로 한 번에 보낼 수 있는 정보량이 적고 주변신호와 도플러 편이 현상에 많은 영향을 받게 된다 [2]. 이러한 특성 때문에 기존에 사용되던 무선 주파수 기반의 네트워크 프로토콜들은 수중 환경으로의 적용이 어렵다고 판단되어, 이를 위한 다양한 네트워크 프로토콜들이 제안되고 있다.

수중 환경에서의 데이터 수집은 육상에서 보다 시간에 대한 제약을 많이 받기 때문에 수중에서의 시간 동기화는 다양한 응용을 위해 필수적이다 [1]. 그러나 악의적인 공격자에 의해 시간 동기화가 방해를 받는다면 [6, 7] 데이터의 정확성과 신뢰성이 크게 저하될 수 있다. 또한 한정된 전력으로 운용되는 센서 노드에서 부정확한 시간 동기

화로 인해 sleep-wakeup 스케줄이 원활하게 작동하지 않는다면 네트워크의 수명이 크게 저하 될 수 있다는 문제가 있다.

본 논문에서는 지금까지 제안된 수중 센서 네트워크의 시간 동기화 프로토콜과 기존 육상에서 사용되는 시간 동기화 보안 기법에 대해 살펴보고 이들 보안 기법의 수중 센서 네트워크로의 적용 가능성에 대해 살펴본다.

II. 관련 연구

본 장에서는 시간 동기화의 필요성과 기존에 사용되는 시간 동기화 기법 및 보안 위협에 대해서 설명하고, 시간 동기화 보안을 위해 제안된 두 가지 기법에 대해 살펴본다.

1. 센서 네트워크 시간 동기화의 필요성 [1]

센서 노드는 내부의 오실레이터로 수정 발진자를 사용한다. 수정 발진자는 휨(skew)과 표류(drift)의 특성으로 인해 1-100us/s의 오차를 가진다 [1]. Mica2 모트의 경우 최대 오차가 4.75us/s까지 발생할 수 있고, 이러한 오차는 1시간이 지나면 17.1ms, 58시간 정도가 흐르면 1초 이상의 차이가 나게 된다. 따라서 다수의 노드들로부터 정확한 결과를 얻어내기 위해서는 노드들 간의 주기적인 시간 동기화가 필수적으로 요구된다.

2. 육상 센서 네트워크 시간 동기화 기법-TPSN(Time synchronization Protocol for Sensor Networks) [4]

그림 1의 TPSN은 제한된 리소스를 가진 센서 노드로 이루어진 무선 센서 네트워크를 위해 제안된 가장 대표적인 시간 동기화 프로토콜이다. TPSN은 노드의 수가 증가하더라도 네트워크 전체의 시간 동기화 정확도가 저하되지 않도록 설계되었고, RBS (Reference Based Synchronization) [5]와 같은 소규모 동기화 프로토콜에 비하여 네트워크 전체 레벨의 동기화가 가능하다는 점이 장점이다. 본 프로토콜은 *level discovery phase*와 *synchronization phase*로 구성된다.

Level discovery phase: 초기에 한 루트 노드가 level 0으로 정해진 후, 루트 노드를 중심으로 송신자의 level과 ID를 담고 있는 level-discovery 패킷을 전파시킴으로써 전체 네트워크에 계층적인 레벨 구조를 구축한다.

Synchronization phase: 두 노드 간에 시간 소인(time stamp) 메시지 교환을 통해 시간차를 계산하고 보정한다.

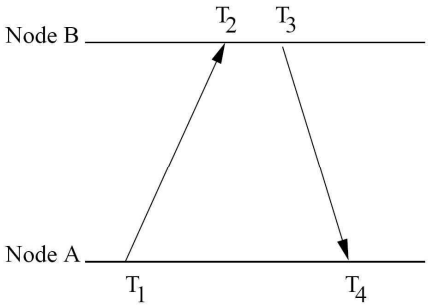


그림 1: 노드간 시간 소인 메시지 교환

$$\theta = \frac{(T2-T1)-(T4-T3)}{2}, \delta = \frac{(T2-T1)+(T4-T3)}{2} \quad (1)$$

수식 (1)은 그림 1에서 측정된 4개의 시간 값을 이용하여 두 노드 간의 시간 편차와 전달 지연을 구하는 수식이다. 여기서 θ는 두 노드 간 시간차를, δ는 메시지 전달 지연을 나타낸다. 수식 (1)을 사용하여 시간차와 전달 지연을 계산할 수 있고, 자신의 지역 시간을 θ만큼 보정함으로써 자신의 지역 시간을 상대노드에게 동기화 시킬 수 있다.

3. 시간 동기화 기법에 대한 공격

1) Pulse-delay attacks [6]

위에서 제안된 TPSN에 대한 공격으로 pulse-delay공격이 제시되었다. 악의적인 공격자는 노드 A가 시간 동기화를 시작하기 위해 노드 B로 송신하는 initial synchronization pulse 패킷에 대해 재밍 (jamming)을 시도하여 전달 시간을 늦춘다. 그 후에 공격자는 일정한 시간이 지난 후에 initial synchronization pulse 패킷을 노드 B에게 전송한다. 이 경우 공격자가 정한 임의의 딜레이 시간 Δ이 추가되므로 수식 (2)에서 볼 수 있듯이 동기화 프로토콜은 올바른 시간 편차를 계산해내지 못하게 된다.

$$\theta = \frac{(T2-T1)-(T4-T3)+\Delta}{2}, \delta = \frac{(T2-T1)+(T4-T3)+\Delta}{2} \quad (2)$$

2) 탈취 노드의 메시지 변조 공격 [7]

외부에서의 메시지 위변조는 암호학적 기법을 사용하여 막을 수 있다. 그러나 악의적인 공격자에 의해 노드가 탈취될 경우, 노드의 비밀 정보가 공격자에게 노출되어 공격에 악용될 수 있다. 시간 동기화 프로토콜 수행 시에 탈취된 노드가 고의적으로 잘못된 시간 소인 정보를 네트워크에 전파시킨다면 정확한 시간 동기화가 이루어지지 않게 된다. 이는 암호학적 메시지 인증 기법을 사용하더라도 막을 수 없다는 어려움이 있다.

4. 보안을 고려한 시간 동기화 프로토콜

1) Ganeriwal et al. [6]

Secure Pairwise Synchronization (SPS)

1. A($T1$)→($T2$)B: $A,\ B,\ N_A,\ sync$
2. B($T3$)→($T4$)A: $B,\ A,\ N_A,\ T2,\ T3,\ ack$

$$MAC_{K_{AB}}[B, A, N_A, T2, T2, ack]$$

3. A calculates delay $d=\frac{(T2-T1)-(T4-T3)}{2}$

$$If\ d \le d^{*}\ then\ \delta=\frac{(T2-T1)-(T4-T3)}{2}\ else\ abort$$

노드간의 시각 동기화에 대한 악의적인 공격을 탐지하기 위해 Secure Pairwise Synchronization (SPS) 프로토콜 [6]이 제안되었다. SPS 프로토콜에서는 사전에 노드에 분배된 비밀 키가 있다고 가정하고, 외부 공격자에 의한 공격에 대해서 각 노드에 분배된 비밀 키를 이용하여 Message Authentication Code (MAC)를 생성하여, 외부 공격자가 synchronization pulse나 ACK 패킷을 변조하는 것을 막는다. 또한 비밀 키 정보를 가지고 있지 않은 외부 공격자가 노드 B를 가장하여 메시지를 보내는 것을 막아주고, nonce값을 사용하여 재생 공격을 막는다. 노드 탈취에 의한 내부 공격자의 pulse-delay 공격에 대해, SPS는 종단간 지연 값과 통계적으로 산출된 종단간 지연의 평균값의 비교를 통해 공격을 탐지한다.

SPS는 노드 간 링크의 종단 간 지연을 통계적으로 측정한 후 표준 편차를 적용한 최대 및 최소 지연 시간을 산출한다. 만약 프로토콜에서 계산된 지연 시간이 위에서 측정된 정상적으로 발생할 수 있는 지연의 범위를 넘어선다면 노드는 공격을 탐지하고 프로토콜을 중지한다. SPS 프로토콜은 공격을 탐지될 시에 프로토콜을 중단하기 때문에 악의적인 공격이 계속 이어질 경우 서비스 거부 공격으로 이어질 수 있다.

2) Kun et al. [7]

Kun et al [7]은 센서 네트워크의 모든 노드들이 공통의 소스, 즉 정확한 시간을 유지하는 외부 시간과 동기화하는 방식을 사용한다. 각 노드들은 외부 시간과의 중복적인 동기화를 통해 부분적인 패킷 손실이나 변조된 시간 소인의 영향에 대해 탄력성(resilience)을 가진다. 위의 아이디어를 기반으로 하여 *level-based clock synchronization*과 *diffusion-based clock synchronization*이 제안되었다. 전자는 계층구조를 구축한 다음 레벨 별로 시간 동기화를 수행하는 방식이고, 후자는 이미 동기화 한 노드들이 그 이웃들에게 다시 동기화를 수행하는 방식이다.

Kun et al은 한 노드가 주위에 적어도 2t+1개의 이웃을 가지고 있고 모든 이웃들과의 시간차의 평균을 계산하여 시간 동기화를 수행한다면 그 중에 고의적으로 잘못된 시간 소인을 제공하는 t개의 탈취된 노드가 존재한다고 하더라도 올바른 시간 동기화를 수행할 수 있다는 장점이 있다.

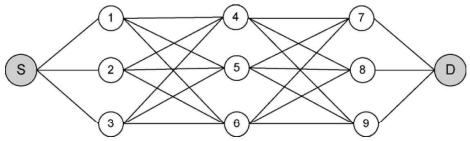


그림 2: 노드 S와 D사이의 메시 네트워크

그림 2에서 S는 외부의 정확한 외부 시간과 동기화한 참조 노드이고, D는 S와 시간 동기화하려는 타겟 노드이다. 두 노드 i와 j간의 시간차를 $\delta_{i,j}$, 각 노드의 지역 시간을 C_i라고 할 때, $\delta_{i,j}=C_j-C_i$로 나타낼 수 있다. 노드 1, 2, 3은 각각 $\delta_{1,s},\delta_{2,s},\delta_{3,s}$를 계산한다. 그 다음, 노드 4는 노드 1, 2, 3을 통해 $\delta_{4,s}$를 획득한다. 노드 1을 통할 경우, $\delta_{4,s}^{(1)}=\delta_{4,1}+\delta_{1,s}$로 시간차를 계산할 수 있고 $\delta_{4,s}^{(2)},\delta_{4,s}^{(3)}$도 같은 방법으로 구할 수 있다. 노드 4는 앞에서 구해진 3가지 값을 평균을 자신과 S의 시간차로 얻음으로써 노드 1, 2, 3중에 탈취된 공격자 노드가 있다고 하더라도 그 효과를 제거할 수

있다. 이와 같은 과정이 노드 7, 8, 9에서도 연쇄적으로 일어나서 노드 D는 노드 S와의 시간차를 계산하여 자신의 시간을 보정할 수 있다.

III. 수중 센서 네트워크를 위한 시간 동기화 기법

본 장에서는 수중 센서 네트워크의 특징에 대해서 살펴보고 수중 음향 센서 네트워크를 위해 제안된 두 가지 시간 동기화 기법, TSHL과 MU-Sync에 대해 살펴본다.

1. 수중 음향 센서 네트워크

수중 음향 센서 네트워크는 사람이 직접 탐사하기 힘든 수중 환경에 배치되어 데이터 수집, 감시 정찰 및 해저 탐사 등에 이용될 수 있다. 그림 3에서와 같이 구체적인 응용으로는 해양 생태계 환경 조사, 해저 침입 탐사, 지진 발생 유무 식별, 오염 물질 분석, 해양 생물 서식 분포 탐사 등 다양한 분야에 활용될 수 있다. 그림 3은 수중 음향 센서 네트워크의 배치 구조를 보여준다.

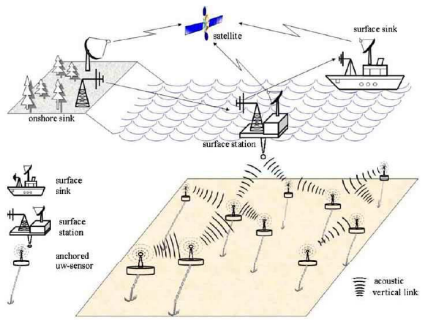


그림 3: 수중 센서 네트워크 구조도

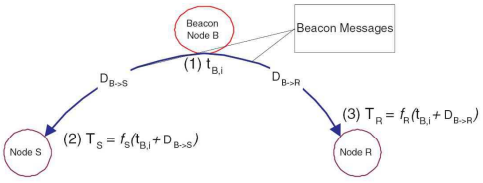
2. 수중 환경의 특성

수중 센서 네트워크는 강이나 깊은 바다에 설치되어 수중 탐사, 재해 방지, 무인 감시 시스템 등의 응용으로 이용이 가능하다. 그러나 기존의 무선 주파수 통신은 수중에서는 심각한 감쇠 현상 때문에 사용하기 어렵다. 그래서 주로 음향 통신을 사용하게 되는데 음향 통신은 약 1500m/s의 속도를 가지므로 큰 전파 지연시간을 가지고 제한된 대역폭을 가지므로, 전송할 수 있는 정보량에 한계를 가진다 [2, 3].

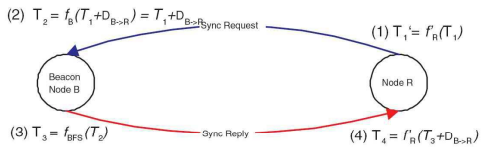
이러한 특성 때문에 기존의 육상에서 사용하던 네트워크 프로토콜은 수중 센서 네트워크에 그대로 적용하기가 힘들다. 시간 동기화 프로토콜 역시 음향 통신의 특성으로 인한 긴 지연시간에 영향을 받게 되므로 수중 환경에 맞는 시간 동기화 프로토콜의 설계가 요구된다.

3. Time Synchronization for High Latency channels (TSHL) [8]

그림 4는 TSHL [8]의 각 단계에서의 메시지 교환을 보여준다. 단계 1에서 비컨 노드의 브로드캐스트 범위 내에 있는 각 노드들은 자신의 클록 휨(skew)를 모델링한다. 비컨 노드는 기준 시간이 되는 클록을 가진 노드라고 정의한다. 비컨 노드는 skew 산출을 위해 충분한 비컨 메시지를 전송한다. 모델링을 위한 선형 회귀분석을 위해 제안 방식에서는 25개의 비컨 메시지가 필요하다.



[단계 1]



[단계 2]

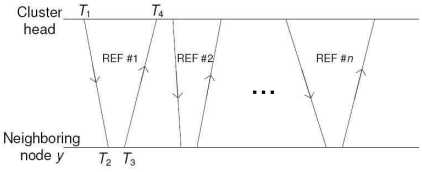
그림 4: TSHL의 시간 동기화 단계

각 비컨 메시지는 Medium Access Acontrol (MAC) 레이어에서 생성된 시간 소인을 담고 있고 수신 노드는 불확실한 전파 지연만큼의 시간 후에 비컨 메시지를 수신하게 되고, 비컨 메시지를 수신한 시간을 자신의 지역 시간(local time)으로 정한다. 이 지역 시간은 클록 skew와 편차(offset), 전파 지연으로 인한 에러가 포함되어 있기 때문에, 앞에서 말한 최소 25개의 비컨 메시지의 시간 소인을 선형 회귀 분석하여 전파 지연과 클록 skew를 정정할 수 있다. skew 정정이 끝난 노드는 주위 노드들에게 Synchronization Request

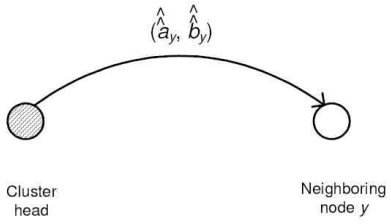
메시지를 전송하고 단계 1에서 전파 지연과 skew를 정정한 후, 단계 2에서는 비컨 노드와의 동기화를 통해 편차를 정정한다. 이는 기존의 TPSN의 synchronization 단계와 동일한 방식으로 수행된다.

4. MU-Sync: A Time Synchronization Protocol for Underwater mobile sensor networks [9]

그림 5의 MU-Sync [9]는 *skew and offset acquisition phase*와 *synchronization phase*를 통하여 휨(skew)과 편차를 산출하고 보정하여 노드 간의 drift를 최소화한다. 첫 번째 단계에서 clock skew와 편차는 n개의 참조 (reference) 비컨들의 집합에 대해 두 번의 선형 회귀분석을 수행하여 산출된다. 여타의 시간 동기화 알고리즘들이 skew를 구하기 위해 한 번의 선형 회귀분석을 적용하는 반면, MU-Sync는 두 번을 수행한다. 첫 번째 회귀분석은 클러스터 헤드로 하여금 REF 패킷에 의해 측정되는 전파 지연에 대해 수행된다. 그 후에, skew와 편차에 대해 두 번째 회귀분석이 이루어진다.



[skew and offset acquisition 단계]



[synchronization 단계]

그림 5: MU-Sync의 시간 동기화 단계

MU-Sync는 클러스터 기반이기 때문에 모바일 멀티-홉 수중 센서 네트워크로의 적용이 용이할 것이라 예상된다. TSHL과 비교해볼 때, 각 노드가 자신의 skew와 편차을 산출하는 방식에 비해 MU-Sync에서는 클러스터 헤드가 그 작업을 수행하기 때문에 전체 네트워크 비용 면에서 절감이 예상된다.

IV. 제안된 프로토콜의 안전성 및 수중 적용 가능성 분석

본 장에서는 시간 동기화 프로토콜에 대한 공격과 방어 기법의 수중 환경에서의 적용 가능성 여부에 대해 알아본다.

1. 큰 전파 지연의 영향

수중 센서 네트워크를 운용함에 있어서 큰 어려움 중 하나가 큰 전파 지연이다. 무선 주파수 통신을 사용한 시간 동기화에서는 전파 지연이 무시할 수 있는 정도로 작지만, 물을 매질로 하는 음향 통신에서는 전파 지연이 매우 크다. 때문에 TSHL과 MU-Sync에서는 다수의 참조 (Reference) 패킷을 통해 선형 회귀 분석을 수행하여 전파 지연의 영향을 최소화한다. 그러므로 pulse-delay attack과 같이 공격자가 임의의 딜레이 시간을 정해서 sync 패킷을 딜레이 한다고 하더라도 그 영향은 선형 회귀 분석에 의해 효과가 사라지게 된다.

또한 전송 지연의 통계적 분석을 활용한 Ganeriwal et al. [7]은 전송 지연이 길고 채널비대칭성 [2]으로 인해 불규칙한 지연 시간을 가지는 수중 링크의 특성 상 정확한 통계적 분석 수치를 얻기 힘들거나 지나치게 넓은 경계 값을 가지게 되어 공격자 판별에 의미를 가지지 못할 것이다.

2.노드의 이동성 및 배치

노드가 고정되어 있는 육상 센서 네트워크와 달리 수중 센서 노드들은 해저 바닥에 완전히 고정된 노드를 제외하고는 센서 노드가 해류 등으로 인해 심하게 이동한다. 또한 비용과 관리 면에서 수중 센서 네트워크는 육상 센서 네트워크만큼 조밀하게 배치되지 못한다. 그러므로 Kun et al.의 논문에서 제시된 주위 노드들과의 편차 평균 계산을 통하여 이상값 (outlier)의 악영향을 줄이는 방식은 사용하기 어렵다. 임계값 이상의 노드 수를 충족시킨다고 하여도, 해류의 이동성으로 인해 배치 형태가 자주 바뀌기 때문에 주위에 노드가 존재하지 않을 경우에는 이상값의 효과가 그대로 전파될 수 도 있다.

3. 향후 수중 시간 동기화에 대한 공격 전망

현재까지 수중 시간 동기화에 대한 효과적인 공격 방법은 제시되지 않고 있다. 시간 동기화에 대한 공격 방식을 외부 공격과 내부 공격으로 나누어 보았을 때 메시지 위변조 등의 공격은 암호학적 기법들을 사용하여 방어가 가능하다. 때문에 육상 시간 동기화에서는 내부 공격이 위협이 되어왔지만 높은 압력으로 인해 사람이 직접 들어가기 힘들다는 점이 노드 탈취에 대한 위협을 크게 줄이고 있다.

그러나 최근에 많은 연구가 진행되고 있는 AUV (Autonomous Underwater Vehicle)의 활용에 따라 다양한 공격 방법이 가능할 것이라 예상된다. AUV는 수중에서 원격 조정을 통해 자유롭게 이동이 가능한 수중 탐사 로봇이다. 이런 장비를 사용하여 TSHL이나 MU-Sync에서 reference 타임을 제공하는 비콘 노드나 클러스터 헤드들에 대하여 물리적 공격이 이루어진다면 작게는 시간 동기화의 정확성을 낮추는 데서 시작하여 전체 시간 동기화를 방해할 수도 있을 것이다.

V. 결론

본 논문에서는 수중 센서 네트워크 응용에서 필수적으로 연구가 요구되는 시간 동기화 프로토콜에 대해 살펴보았다. 지금까지 TSHL과 MU-Sync와 같은 수중 시간 동기화 프로토콜이 제안되었지만 아직 수중에서의 보안을 고려한 프로토콜들은 제안되고 있지 않다. 이에 본 논문에서는 기존의 육상 센서 네트워크에 존재하는 시간 동기화에 대한 공격 방법들과 방어 기법들에 대해 살펴보고 이를 수중에 적용했을 때의 적용 가능성 여부에 대해 살펴보았다.

참고문헌

[1] B. Sundararaman, U. Buy, A.D. Kshemkalyani, "Clock synchronization for wireless sensor networks: a survey", *Ad Hoc networks* 3(3), pp. 281-323, 2005.

[2] M. Stojanovic, "Acoustic (underwater) Communications", In *J.G. Proakis editor, Encyclopedia of Telecommunications. John Wiley and Sons*, 2003.

[3] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater Acoustic Sensor Networks: Research Challenges", *Ad Hoc Networks (Elsevier)*, 3(3), pp. 257-279, May 2005.

[4] S. Ganeriwal, R. Kumar, M. B. Srivastava, "Timing-sync protocol for sensor networks", Proceedings of the 1st international conference on Embedded neetworked sensor systems, pp. 138-149, Nov 2003.

[5] J. Elson, L. Girod and D. Estrin, "Fine-Grained Network Time Synchronization using Reference Broadcasts", *Proc. Fifth Symposium on Operating Systems Design and Implementation (OSDI) 2002),* Vol 36, pp. 147-163, 2002.

[6] S. Ganeriwal, Srdjan Capkun, Chih-Chieh Han, and M. B. Srivastava, "Secure time synchronization service for sensor networks", *WiSe '05:Proceedings of the 4th ACM workshop on Wireless security,* pp. 97-106, 2005.

[7] Kun Sun, Peng Ning and Cliff Wang, "Secure and resilient clock synchronization in wireless sensor networks", *IEEE Journal on Selected Areas in Communications,* 24(2), pp. 395-408, 2006.

[8] A. Syed and J. Heidemann, "Time Synchronization for High Latency acoustic networks", *IEEE Infocom,* Barcelona, Spain, April 2006.

[9] Nitthita Chirdchoo, Wee-Seng Soh and Kee Chaing Chua, "MU-Sync:A Time Synchronization Protocol for Underwater Mobile Networks", in *Proc. ACM WUWNet,* San Francisco, California, USA, Sep 2008.