International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 5, May-2015, pp: (123-127), Impact Factor: 1.252, Available online at: www.erpublications.com

Secure Co-operation of AURP (An AUV-Aided Underwater Routing Protocol) for Underwater Acoustic Sensor Networks

Reetu Dalal[1], Mrs. Poonam Singal[2], Vinay Agrawal[3]

[1]Deenbandhu Chotu Ram University of Science and Technology, Murthal-131039, Haryana, India
[2]Department Of Electronics and Communication, Deenbandhu Chotu Ram University of Science and Technology Murthal- 131039, Haryana, India
[3]Department Of Computer Science and Technology, YMCA University of Science and Technology Faridabad Haryana, India

Abstract: Security has become one of the essential requirements in any application domain of wireless sensor networks. so that we can send data to authenticated person on a secure channel ensuring all the aspects of security features like confidentiality , integrity , authentication , But it is more essential in domain like underwater acoustic sensor networks since bandwidth is severely limited, energy of sensors is limited and propagation delay is very high and hence we have limited resources that must be utilized efficiently .In order to address those challenges the work proposes a mobile agents based architecture of secure co-operation of AURP (An AUV-aided underwater routing protocol) with objective of maximum data delivery and minimum energy consumption . Further these mobile agents are encrypted and embedded in AUVs in there buffer for the data capture process as these mobile agents can travel the network through controlled AUV's. The work uniquely contributes a mobile agent based periodic approach for collecting data from various gateway nodes (cluster heads) of different clusters as specified in its itinerary using travelling sales person so that it covers all of them using optimal energy & processing them one by one and completing its itinerary and deposit the data to sink and then repeat the same process again periodically when these AUVs gets charged exploiting solar energy. Each cluster have some members within one hop distance that have sensed data which need to be sent to gateway node using encrypted mobile agents only when AUV's services to that particular gateway node.

Keywords: Wireless sensor networks, Mobile agents, AUV, AURP.

Introduction

Wireless sensor networks are having many application domains for terrestrial and underwater space. Our main focus is on underwater application domains, where we use underwater acoustic (sound) sensor networks. Since radio waves could not be exploited in deep water hence we use sound waves (acoustic waves) for transmitting data. Underwater sensor networks have vast variety of applications like pollution monitoring, underwater explorations, surveillance and patrolling application etc. Each of the application can make use of a efficient protocol intended for that application. Many latest research works shows implementation of different protocols for underwater applications, protocols using software agents etc., but still they are not perfect because of the physics of underwater like high propagation delay, path loss, limited bandwidth etc.

Now a day's underwater acoustic network are using Autonomous underwater vehicles (AUV's) or unmanned underwater vehicles , that can move from one place to another collecting data from all the nodes in its vicinity and depositing to the base station. They are having high resources and can't be compromised sooner, they can also be recharged using solar energy when they gets discharged (after coming to surface water). Current research trends on underwater acoustic networks shows the use of software agents for minimum consumption of energy and maximization of output and hence extending the life time of the monitoring system.

In computer science, a systems agent is a computer program that acts for a user or other program in a relationship of agency, which derives from the Latin agere (to do): an agreement to act on one's behalf. Such "action on behalf of" implies the authority to decide which, if any, action is appropriate.

As we know that security has become one of the essential requirement now a days for any application domain. Security is also required in underwater applications because of the nature of the underwater environment and limited bandwidth that must be properly utilized .Underwater environment presents a variety of challenges like path loss , limited bandwidth , multipath , propagation delay etc . Without security a malicious node can make use of these limited resources and could result in Daniel of services attack or loss of energy resources which is supposed to be very precious asset for our monitoring system.

Related Work

Current research work shows that mobile agents are playing crucial roles in Wireless Sensor Networks and the task of injecting mobile agents in WSNs has been extremely attracting researchers and persons from organizations in latest times. Following Section shows the work of well-known researchers in this field.

[Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal] gave a top down overview of several new applications and review the literature on various aspects of WSN. they classify the problems into 3 different categories :(1) Internal platform and underlying operating system,(2) Communication protocol stack (3) Network Services, provisioning and deployment .**[Geoffrey A. Hollinger, Urbashi Mitra, and Gaurav S. Sukhatme]** examine the planning path problems that an AUV confronts when collecting data, AUV must move in such a fashion that it covers all the required nodes in minimum time and least energy and fuel using traveling salesperson , they extended approximation algorithms for variants of Travelling salesperson problem .**[Ian F. Akyildiz *, Dario Pompili, Tommaso Melodia]** discussed 2-D and 3-D architectures of Underwater network, characteristics of underwater channels , challenges for development of effective networking solutions posed by physics of underwater.

[**Seokhoon Yoon, Abul K. Azad, Hoon Oh, and Sunghwan Kim]**proposeda AURP(AUV-aided underwater routing protocol) , which uses heterogeneous acoustic communication channels and controls the mobility of AUV's . In this protocol the total data transmissions are minimized using AUVs as relay nodes , they collects the sensed data from all the cluster heads as specified in their trajectory and deposit it to sink node . It's a multi AUV platform , where mobility of AUV's is controlled using mobile agents and the results shows the maximization of data delivery ration and minimization of energy consumption.**[Andrea Caiti, Vincenzo Calabr`o, Gianluca Dini , Angelica Lo Duca and Andrea Munaf`o]** gave methodologies and cooperative algorithms for secure cooperation of a group of AUV's nodes that are sensing the data near a high value asset(base station) and protecting the High value Asset .These algorithms are robust and flexible . They implemented integration between security suite and cooperative algorithm and provides the statistics results.**[Md. Ahasan Habib, Jia Uddin, Md. Monirul Islam]** said that UASN are susceptible to malicious attacks coz of the high transmission power requirements, rapidly changing channel characteristics , multi -path echoes , high bit error rates, propagation delays etc. They presents an analysis for safety measurements for underwater networks and research challenges for secure communication between UASN and ground based counter parts.

3. Secure Co-operation of AURP: The Proposed Work

As mentioned in the previous section, AURP is the backbone of this work. The proposed work focuses on data encryption. This work mainly caters periodic applications. When the AUV visits the cluster head, it transfers an encrypted agent to it which is encrypted using AUV's private key. Now that agent after receiving from AUV at cluster head decrypted using the public key of AUV and encrypted with the cluster-head private key . Now that encrypted agent is forwarded to all the cluster members of that cluster-head. These all sensor nodes now decrypts that agent using cluster-head public key and gets the information. The information can be the requirement of the sensed data from them depending on the application. Hence these sensors now encrypts the needed data as asked in information using their own private keys and forwards back to the cluster-head simultaneously. The cluster-head concatenates all the encrypted data and further encrypts that whole data using his own private key and dispatch whole data set of that cluster-head back to the AUV. AUV have the public key of all nodes of its domain it is servicing for, and hence decrypts the data in reverse fashion that is decrypting by cluster-head public key and them the keys of member node of that cluster one by one or simultaneously on all the encrypted data chunks and gets the individual results that is stored in its memory. Now it moves to 2nd cluster-head and repeats the same process to it and in this way it completes the whole trajectory and deposit all the data to sink (base station) . This Process is repeated periodically to gather the real time data. For the next cycle of the process we could use another AUV and in same time the exhausted AUV can be recharged exploiting solar energy and can be used in next cycle and so on. In this way whole monitoring process is distributed to different areas within which works independently resulting the whole monitoring process which is real time and secure specially for surveillance and patrolling applications

3.1 High Level View of Secure AURP

Secure AURP is a periodic protocol which presents a hierarchical solution in a clustered sensor network. The work proceeds by adopting a key management system which introduces various set of keys for encryption/ decryption. The high-level view of the proposed work is depicted in figure 1.The fundamental backbone remains AURP i.e. mobile agents are embedded on to AUV's. The extensive secure protocol have a group controller for each set of cluster-heads and AUV , which have two main components i.e. key management service(KMS) and secure dispatching service (SDS). KMS is used for periodic rekeying for a particular set of cluster-heads with their AUV independently. Each time before an AUV starts its cycle a periodic rekeying is done i.e. all the nodes are assigned new keys to all cluster-heads , their members and to the AUV both public and private keys to each then the AUV completes its operation in its trajectory by exchanging information and data using secure dispatching service(SDS) . Now when AUV want to go for next cycle after some period then it will again have to call KMS to assign new keys to all the sensors. This periodic rekeying is done at the aim of amount of encrypted information is limited with the same key is only gets available to an adversary, only if he gets that key through some passive/active attacks. Hence theses keys will be changed at each cycle. Now SDS provides secure dispatching of information/data to or from by encrypting/decrypting it first then forwarding it. Hence is ensures the basic security features like confidentiality, integrity and authenticity.

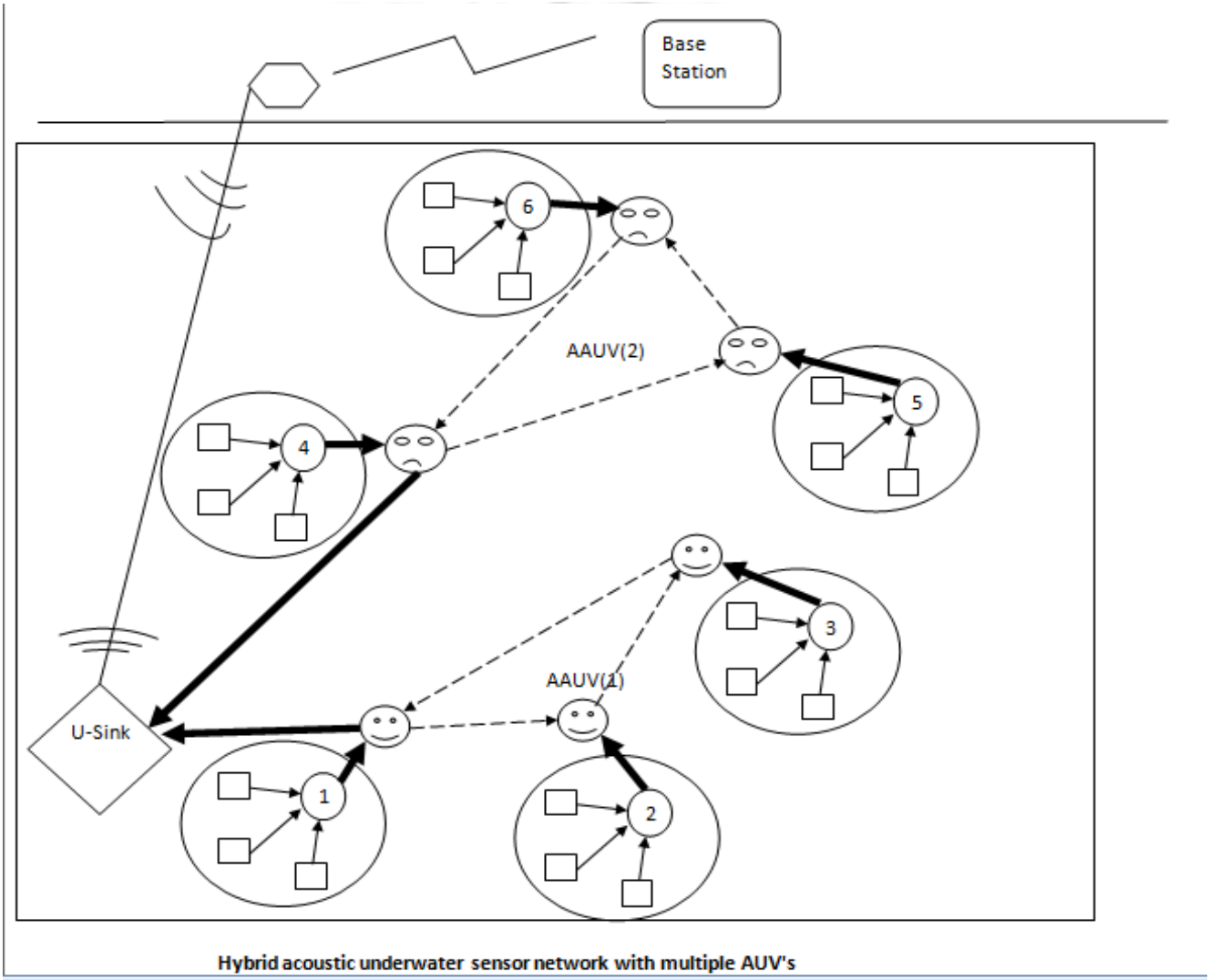

Fig 1: High Level View of Proposed Work

SDS implements the cryptographic transformations applied to network traffic segments. Theses transformations specifies the cryptographic processing applied to message before sending or after receiving them .For Example, in order to ensure both confidentiality and integrity of a message, a possible transformation is Ee(mkh(m)), where E specifies a symmetric cipher, h specifies an hash function and e is an encryption key. Whereas, a transformation aimed at ensuring only authentication of message m ismkHa (m), where a is an authentication key and H is a Message Authentication Code (MAC).

3.2 Algorithm

Input: Sensors are deployed and clusters get formed dynamically and they continuously senses the data. Cluster-heads are assumed.
Source list //sequence of all cluster head sensor nodes
first_source //first cluster-head where agent is dispatched initially
last_source //destination cluster-head node.

Output: P_agg_data // Aggregated and processed pressure value at sink

Steps:

Step 1 If Node is AUV Node
For All AUV Nodes in Network
Broadcast ADV message to cluster heads that it is AUV node
Receive Join requests
Assign Src_List, First_src, Last_src in that AUV node buffer memory (Assigning its trajectory)

Step 2 If Node is cluster-head node
Wait for ADV Messages from AUV's
Receive ADV join request
Send join request to best AUV Near by

Step 3 for All AUV Nodes in Network
For All cluster-heads of that AUV i
For All Members of that Cluster-head j
Call Key_Management_Service ();
// Public and private keys for all the sensors & AUVs gets generated

Step 4 for All AUV Nodes in Network
For All cluster-heads of that AUV i
AUV goes for jth cluster head and dispatch encrypted agent using his private key through Secure dispatching service (SDS)
Now cluster-head decrypts it using the AUV's public key after receiving through SDS and encrypts with his own private key
For All members for the cluster head j
Dispatch that encrypted agent to all the members of the cluster
All the members decrypts the message using public key of cluster-head j and encrypts the required sensed data using their own private key and forwards back to cluster head
Cluster-head j further encrypts it using his own private key and forwards back to AUV i.
Repeat

Step 5 Now All AUV nodes have aggregated data of all their respective set of cluster-heads , which is deposited to the sink.

Step 6 Take appropriate actions if required based on data collected.

Step 7 Repeat from step 5 to step 8 periodically for All AUV's

4. Conclusion and Future work

In a resource constrained environment like underwater wireless sensor network the current approach has been able to suggest a novel approach for security. This approach has made use of mobile agents for transmitting the data in a secure manner. Though this approach has been able to effectively deal with the issue of security, the problem of the scalability of the network and its robustness still need to be dealt with.

There are certain issues which needs to be addressed by further research related to secure cooperation in underwater wireless sensor networks. The first issue which needs to be addressed is scalability of the network. Though the approach is working fine for a small network, its working when the network size grows still needs to be tested. Further, the effect of water currents on the AUV's and cluster-heads has not been considered in the current work. The authors aim to do the same in their future research work.

References

[1]. Jennifer Yick; Biswanath Mukherjee; Dipak Ghosal (2008) “Wireless sensor network survey" Journal of computer Networks, 52, pp 2292-2330.
[2]. Geoffrey A. Hollinger; Urbashi Mitra; Gaurav S. Sukhatme " Autonomous Data Collection from Underwater Sensor Networks using Acoustic Communication".
[3]. Ian F. Akyildiz; Dario Pompili; Tommaso Melodia (2005)" Underwater acoustic sensor networks: research challenges" Journal of Ad hoc Networks, 3, pp 257-279.
[4]. Seokhoon Yoon; Abul K. Azad; Hoon Oh; Sunghwan Kim (2012) "AURP: An AUV-Aided Underwater Routing Protocol for Underwater Acoustic Sensor Networks" Journal of Sensors (Basel),12(2),pp 1827-1847.
[5]. Andrea Caiti; Vincenzo Calabr`o; Gianluca Dini; Angelica Lo Duca; Andrea Munaf`o (2012)" Secure Cooperation of Autonomous Mobile Sensors Using an Underwater Acoustic Network” Journal of Sensors, 12, pp 1967-1989.
[6]. Md. Ahasan Habib; Jia Uddin; Md. Monirul Islam (2012) "Safety Aspects of Enhanced Underwater Acoustic Sensor Networks" International Journal of Emerging Technology and Advanced Engineering,2, pp 2250-2459.