2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)
IPCSIT vol. 53 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V53.No.1.06

Secure and Reliable Multi-Path Transmission Scheme on Underwater Acoustic Sensor Networks

ZHANG Mei-Yan[1+], CAI Wen-Yu[2] and ZHANG Hong-Tao[3]

[1]Zhejiang Water Conservancy and Hydropower College, Hangzhou 310018, China
[2]School of Electronics & Information, Hangzhou Dianzi University, Hangzhou 310018, China
[3]State Key Laboratory of Sonar Technology, Hangzhou Applied Acoustic Research Institute

Abstract. Underwater Acoustic Sensor Networks (UASN) based on the advances in underwater data collection and observing systems may play an important role in oceanographic research. But many unique features of UASN pose challenge on development of reliable and secure data transport to overcome harsh aquatic communication conditions. In this paper, we use multi-path routing to address secure and reliable transmission issue named as SRMR. There are two contributions in the area of secure and reliable transmission control protocols for UASN: (1) Forward Error Correction (FEC) erasure coding employed in multi-path routing is used to guarantee reliable transmission resistant to frequent acoustic error; (2) Weighted Threshold Secret Sharing (WTSS) is used to guarantee secure transmission resistant to malicious attack, and one message is split into multiple shares and then delivers the message shares to the sink node via multiple independent paths instead of using single one path. Recent researches have addressed secure transmission or reliable transmission scheme but these two aspects are independent, therefore, to our knowledge, design a secure and reliable compatible routing scheme for UASN is the first research in publish. Therefore, our proposed SRMR scheme provides a novel approach to guarantee reliable and secure transmission in harsh acoustic communication channel. The results verified the performance of this proposed SRMR scheme through simulation, and the simulation confirms the result from analytical study.

Keywords: Underwater Acoustic Sensor Networks (UASNs); Multi-path Routing; Weighted Threshold Secret Sharing (WTSS); Secure Routing; Forward Error Correction (FEC)

1. Introduction

Underwater Acoustic Sensor Networks (UASN) [1-3], which has received growing interests recently, has many potential underwater monitoring applications such as seismic imaging of undersea oilfields, oceanographic data collection and disaster warning because the prefect scalability of UASN ensures that large interest underwater or oceanic areas can be covered for time-critical applications. Therefore, UASN is becoming increasingly important for oceanographic and other monitoring applications, therefore, it empower us to explore deeper into our underwater world.

However, different from terrestrial sensor networks, UASN has the following unique characteristics [4]: limited acoustic bandwidth capacity, extreme propagation delay, high deliver error probability, severely limited energy constraints, time-varying severe inter-symbol interference, large Doppler shifts, sensor nodes' passive mobility [5] and etc. All these features pose challenge on development of networking protocols to overcome harsh communication conditions, one of the major challenges in UASN is reliable and secure data transport.

+ Corresponding author.
E-mail address: Meiyan19831109@163.com.

In UASN, multi-hop relay transmission manner is used to deliver acquired data from sensor nodes to the sink node. In underwater environments, wireless radio does not work well due to extremely limited propagation distance, thus acoustic channels are usually employed. However, due to the long propagation delay and high error rate of acoustic channels, it is very challenging to provide reliable data transfer in an energy-efficient way.

Reliable transmission problem of UASN is to solve how to improve successful delivery ratio as possible as can when transmitting sensing information to the sink node [6]. Since acoustic links of UASN are susceptible to different kinds of interferences and are prone to failure caused by energy exhaustion, reliable transmission between sensor nodes to the sink node is hard to be guaranteed.

Secure transmission is a more and more important issue for UASN. When UASN is deployed in a hostile situation, some sensor nodes are prone to be compromised. After some sensor nodes are compromised, many attacks can be taken place frequently such as DoS (denial-of-service) attack, eavesdropping and invasion, spoofed, altered, or replayed routing information, sinkhole attacks, sybil attacks, wormholes, HELLO flood attacks, acknowledgement spoofing etc [7].

Combination reliability with security together to improve transmission performance of UASN is the main issue addressed for this paper. Security and reliability are two seemingly contradicting objectives [8], because reliability requires more redundancy while security requires less or no redundancy, but in this paper, we dedicate to investigating combination security with reliability with weight secret sharing scheme and redundant erasure coding technology on multi-path routing, which is named as secure FEC (SecFEC) technology.

The remainder of the paper is organized as follows. Section II analyses popular secure and reliable transmission algorithms in detail. In Section III, secure and reliable multi-path transmission algorithm, which is named as SRMR in short, is proposed in detail. Simulation results are provided in Section IV. Finally, Section V concludes this paper briefly.

2. Related Works

It is much more difficult to provide a perfect security solution for UASN due to its distinguished manner and distinguished characteristics such as vulnerability of acoustic channels owing to shared medium, dynamic change of network topology, resource and energy specific limitations, etc.

Most current researches on reliable and secure transmission are concern with WSNs and there are few researches on UASN.

Secure issue on WSNs (Wireless Sensor Networks) has attracted intensive attention in recent years. C. Karlof and D. Wagner [7] enumerated attacks in routing protocols for WSNs and proposed several countermeasures. H. Yih-Chun and A. Perrig [9] enumerated recent secure routing protocols due to four kinds of routing misuses: route disruption, route invasion, node isolation, resource consumption. In Ref. [10] idiographic secure routing schemes and wormhole detection, DoS detection etc. schemes are investigated.

Multi-path routing protocols [11, 12] are resilient to DoS attack and can protect WSNs availability from malicious sensor nodes. The original researches on multi-path routing protocols concern on network load balance mainly. Gradually, scholars found that higher secure delivery ratio can be achieved with multi-path routing [13]. By employing *k*-node-disjoint multi-path between two communication nodes, the routing protocol is resilient against DoS attacks of an adversary that controls less than *k* malicious nodes. Intrusion-Tolerant Routing in Wireless Sensor Networks (INSENS) [14] is a multi-path secure routing that provides protection against routing attacks that spread incorrect control packets containing false routing information through network.

There are a few algorithms proposed for reliable transmission issue on WSNs and UASN [15-18]. PSFQ (pump slowly, fetch quickly) [15] examines the problem of dispensing a wireless sensor network reliably, and make use of hop by hop recovery with caching at intermediate sensor nodes, as opposed to end-to-end recovery. Event-to-sink reliable transport (ESRT) [16], works well for guaranteeing event reliability for event-driven applications that require no packet reliability; however, ESRT is not energy efficient compared to loss

recovery. These reliable transmission schemes are available in particular applications and are not universal. Networking Protocols of UASN are discussed by a few researchers, such as Ref. [17, 18].

In this paper, we use multi-path routing to address secure and reliable transmission issue. There are two contributions in the area of secure and reliable transmission control protocols for UASN. On the one side, forward error correction (FEC) erasure coding is used to guarantee reliable transmission resistant to frequent acoustic error; On the other side, weighted threshold secret sharing is used to guarantee secure transmission resistant to malicious attack, and one message is split into multiple shares and then delivers the message shares to the sink node via multiple independent paths instead of using single one path. Recent researches have addressed secure transmission or reliable transmission scheme but these two aspects are independent, therefore, the main innovation of this paper is to design a secure and reliable compatible routing scheme for UASN.

3. Secure and Reliable Multi-path Routing

3.1 Multi-path Routing

Multi-path routing is an effective strategy to improve the reliability while meeting link failure caused by unreliable acoustic links and frequent network topological changes due to passive current mobility. There are three kinds of Multi-path Routing (MR) protocols as shown in Fig.1.

Node-disjoint MR: The node-disjoint property ensures that, when *k* alternate nodes are constructed, no set of *k* node failures can eliminate all the paths.

Link-disjoint MR: The link-disjoint property ensures that, when *k* alternate paths are constructed, no set of *k* link failures can eliminate all the paths.

Joint MR: The paths in joint multi-path will be shared with common links and common nodes.

Intuitively, multi-path routing algorithms are simple and efficient because no encryption is needed and data is split among different paths to eliminate potential eavesdropping of unauthorized users. With multi-path routing, more data than necessary can be transmitted along different multiple paths concurrently and so that can improve transmission reliability. The base station receives all data slices and then reconstructs the original information to tolerate up to a certain amount of link loss and link eavesdropping. Ultimately, multi-path routing is beneficial to solve secure transmission and reliability transmission problems. In this paper, security over link-disjoint multi-path protocols is investigated.

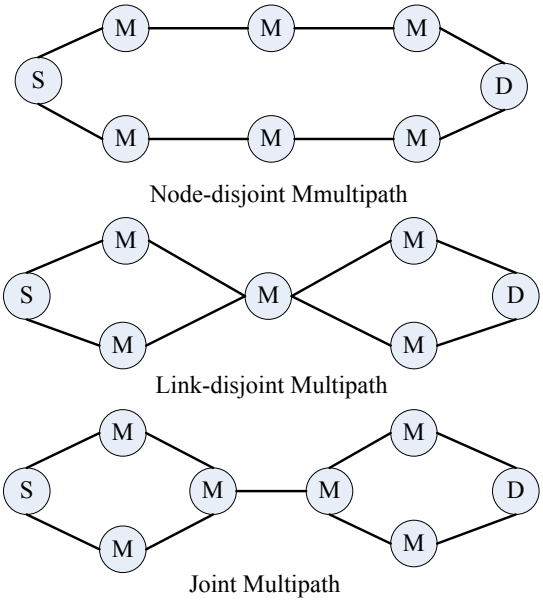

Fig. 1 Category of multi-path routing protocols

3.2 Threshold secret sharing

In this paper, we suppose that once a sensor node is compromised, all secrets stored in that sensor node including cryptographic keys may be compromised, which jeopardized the information relayed to that sensor node. In this paper, we cite threshold secret sharing scheme to guarantee secure transmission on UASN. Threshold secret sharing algorithms [19, 20] could divide a secret into *N* pieces, called *N* shares. From any less than *k* shares one cannot know anything about system secret, while with an effective algorithm, one can reconstruct the system secret from any *k* out of *n* shares. The definitions of threshold secret sharing and weight threshold secret sharing are expatiated below:

Definition1: Threshold Secret Sharing (*k*, *n*)

In threshold secret sharing scheme (*k*, *n*), a secret is divided into *n* segments and is distributed to *n* participators. Any at least *k* participators can cooperate to achieve secret message, otherwise can not.

Definition2: Weighted Threshold Secret Sharing (k, n, ω)

In weighted threshold secret sharing scheme (k, n, ω), different weights are used to give differential influence to participants $u \in U$. If the sum of weights of the participants is as big as or bigger than the threshold value, i.e., $\sum_{u \in U} \omega(u) \geq k$, they can recover the secret, otherwise, $\sum_{u \in U} \omega(u) < k$, they can not, where $\omega(u)$ and U denote the weight value of user *u* and the aggregate of user respectively.

Besides, the details of how to construct weighted threshold secret sharing can refer to Shamior's Lagrange interpolating polynomial scheme [21].

3.3 Redundant erasure coding

Since sensor nodes and acoustic links are prone to failure because of energy exhaustion or malicious attack, the packet loss ratio of acoustic links in UASN is much higher than that of wired or wireless links, and this effect accumulates quickly as the hop number increases. If a message is lost at the p^{th} hop, all previous *p*-1 delivery become wasted effort. With redundant erase coding scheme, we can reconstruct *m* original messages by receiving any *m* out of *n* code words. If *n* is sufficiently large compared to the loss ratio, we can achieve high reliability without retransmission.

Forward Error Correction (FEC) [22] scheme is one of error control schemes suggested for wireless channels. FEC mechanisms are open-loop mechanisms based on the transmission of redundant information along with the original information so that some of the lost original data can be recovered from the redundant information. Therefore, with FEC scheme, the original packet can be correctly recovered even if every individual received copy of this packet is corrupted. The principle of FEC algorithm is shown in Fig.2. The transmitter will use FEC encoding matrix *G* to convert *K* message slices to *N* slices. After transmitting on wireless channel, some packet slices are lost and the receiver has only get *N*' packet slices. With the decoder matrix *G'*, the receiver can recover the original message. These operations mainly comprise of vector arithmetic and matrix inversions. But in Galois field, which is a field with a finite number of members, these operations can be made very efficient with modular operations on finite fields. A prime field is a Galois field *GF*(*p*) whose elements are integers in [0, *p*-1], where *p* is prime. Addition and multiplication are normal integer addition and multiplication with modulo operation in the end. Prime field always have a generator. The size of prime field is *p*, and we need $[\log_2 (p)]$ bits to represent all elements.

Reed-Solomon (RS) [23] code is the most important type of forward error correction codes, which are used for error detection and correction in error control schemes. The basic idea of Reed-Solomon code is to produce *n* equations with *k* unknown variables (*n*>*k*) such that with any *k* out *n* equations, we can find those *k* unknowns. RS code can provide a wide range of code rates, make efficient use of redundancy and efficient decoding techniques are available for use with RS codes.

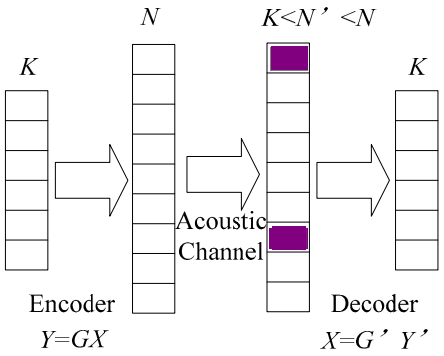

Fig. 2 The principle of FEC algorithm

Vandermonde matrix is used to construct Reed-Solomon code. Vandermonde matrix is a matrix with elements $G(i,j)=\omega_{i-1}^{j-1}$, where each ω_i is nonzero and distinct from each other, as shown in Equation (1). For an n by k Vandermonde matrix ($n>k$), any set of m rows forms a non-singular matrix. For whatever set with k rows we may choose, rows in the set are linearly independent.

$$G_{n\times k}=\begin{pmatrix} 1 & \omega_0 & \omega_0^2 & \cdots & \omega_0^{k-1} \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{k-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \omega_{n-2} & \omega_{n-2}^2 & \cdots & \omega_{n-2}^{k-1} \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{k-1} \end{pmatrix} \tag{1}$$

Reed-Solomon coding process using Vandermonde matrix is a linear equation group, as shown in Equation (2).

$$\begin{pmatrix} Y_0 \\ Y_1 \\ \cdots \\ Y_{n-2} \\ Y_{n-1} \end{pmatrix}=\begin{pmatrix} 1 & \omega_0 & \omega_0^2 & \cdots & \omega_0^{k-1} \\ 1 & \omega_1 & \omega_1^2 & \cdots & \omega_1^{k-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \omega_{n-2} & \omega_{n-2}^2 & \cdots & \omega_{n-2}^{k-1} \\ 1 & \omega_{n-1} & \omega_{n-1}^2 & \cdots & \omega_{n-1}^{k-1} \end{pmatrix}\begin{pmatrix} X_0 \\ X_1 \\ \cdots \\ X_{k-2} \\ X_{k-1} \end{pmatrix} \tag{2}$$

where $G_{n\times k}$ denotes a Vandermonde matrix, X denotes a vector of messages, and code words are contained in a vector $Y(X)=GX$. The polynomial $Y(X)$ using original message slices $X=[X_0,X_1,...,X_{k-2},X_{k-1}]$ as coefficients, such that

$$Y_j(\omega_j)=\sum_{i=0}^{k-1}\omega_j^i x_i \ \ (j=0,1,...,n-1) \tag{3}$$

We then evaluate this polynomial $Y_j(\omega_j)$ at n different points $\omega_0,\omega_1,...,\omega_{n-1}$.

In this paper, secure and reliable transmission for UASN is guaranteed by employing secure FEC scheme, which is derived from combination of Reed-Solomon code with threshold secret sharing scheme.

3.4 SRMR

To facilitate discussion of the secure and reliable multi-path transmission algorithm, we consider a UASN model in which sensor nodes are arbitrarily deployed in a three dimensional aqueous plane. The topology of UASN can be represented by a graph $G=(V(G),E(G))$ in the plane, where $V=\{v_1,v_2,...,v_n\}$ denotes the set of vertices and $E=\{e_1,e_2,...,e_k\}$ denotes the set of edges. $MP(s,d)$ is defined as the set of all possible disjoint paths from s to d, such that,

$$MP(s,d)=\{P_1(s,d),P_2(s,d),...,P_m(s,d)\} \tag{4}$$

A path from source node s to destination node d is defined as $P(s,d)=\{s...d\}$, which is as a sequence of intermediate nodes between node s and node d without loops.

$$P_i(s,d)=\{e_{i1}e_{i2}...e_{ir_i}\} \ \ (e_{ij}\in E(G)\ \forall j\in r_i) \tag{5}$$

Packets Drop Ratio (PDR) of path $P_i(s,d)$ is defined as

$$p_i(s,d) = 1 - \prod_{e_j \in P_i(s,d)} (1 - p_{e_j}) = 1 - \prod_{j=1}^{r_i} (1 - p_{e_{ir_j}}) \tag{6}$$

Packets Malicious Ratio (PMR) of path $P_i(s,d)$ is defined as

$$q_i(s,d) = 1 - \prod_{e_j \in P_i(s,d)} (1 - q_{e_j}) = 1 - \prod_{j=1}^{r_i} (1 - q_{e_{ir_j}}) \tag{7}$$

How to reduce packets drop ratio and packets malicious ratio as possible as can are the main principles in this paper. In addition, we are dedicated to improve these two performances together in spite of any unreliable acoustic links and malicious acoustic links in UASN. Therefore, we can formulate an optimization problem to optimize PDR and PMR while meeting certain energy efficient constraints.

For an underwater acoustic channel, its average path loss is given by [24],

$$A(d, f) = d^{\alpha} \beta(f)^d \tag{8}$$

where d denotes the distance of the acoustic channel; α denotes the spreading factor ($1 \le \alpha \le 2$); and $\beta(f)$ is the absorption coefficient which is determined by the frequency of the acoustic channel f. In this paper, $\beta(f)$ is the same and unique.

The generation of shares is very simple, by evaluating a polynomial of degree (T-1),

$$f(x) = (\alpha_0 + \alpha_1 x + ... + \alpha_{T-1} x^{T-1}) \bmod p \tag{9}$$

At point $x = i$ we can obtain the ith share $S_i = f(i)$, where $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_{T-1}$ are the secret bits, while p is a large prime number greater than any of the coefficients and can be made public. The length of coefficients needs to be one bit shorter than that of p. According to the fundamental theorem of algebra, T values of a polynomial of degree (T-1) can completely determine the polynomial of (i.e., all its coefficients), which any fewer values cannot determine the polynomial (at least computationally difficult). Thus, any T shares can reconstruct the original secret bits, but any fewer shares cannot, and so this is similar to majority voting strategy.

SRMR scheme is based on link-disjoint routing and splits a message into multiple shares using weight secret sharing scheme and then delivers the message shares to the destination via the multiple independent paths.

The data partition and combination in SecFEC scheme is described below: Firstly, dividing one chunk data into M small pieces. Then each piece of data and threshold secrets are divided into K messages, and encoded into N code words together using SecFEC scheme. Then the total number to transmission is MN code words. Pack the i th code words from each independent N data into a single packet. Any K packets will provide K code words for original K data, and we can reconstruct original K data. Since K data have code words with same sequence set, decoding process is the same: the same decoding matrix can be used.

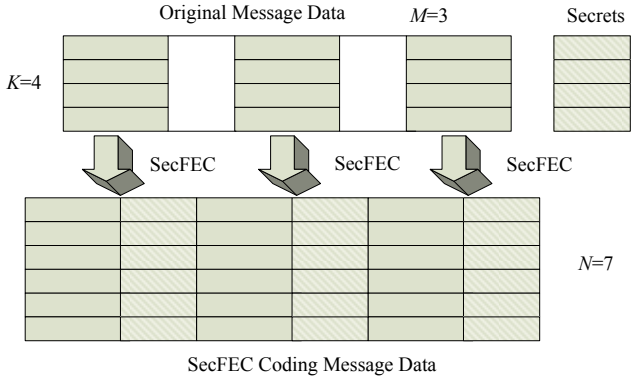

Fig. 3 SecFEC coding scheme

As we know, acoustic communication consumes much more energy than radio communications. In the SecFEC approach, packets are encoded at the sender, and then transmitted continuously to the receiver. At the receiver side, lost packets are ignored, and original data packets can be reconstructed after enough number of encoded packets are successfully received. Apparently, SecFEC will consume much more energy for

redundant transmission. In other words, additional energy is wasted to achieve reliable data transport. However, SecFEC is relatively simple to realize and is much more energy efficient than simple ARQ actually.

4. Simulations

In order to verify the correctness and effectiveness of proposed SRMR algorithm, in this section, we evaluate Packets Drop Ratio and Packets Malicious Ratio of SRMR algorithm. We present a scenario in which N (from 50 to 250) sensor nodes are randomly distributed in a 3D area of 1000^3 meters. Each sensor node has a unified maximal transmission range of 250 meters. Packets drop ratio and packets malicious ratio are randomly distributed with range [0, 0.2] and [0, 0.1] respectively. N-to-1 transmission manner is used in the simulations and the base station is located at the center of 3D region. Obtained by repeated simulations and statistical analysis, the results shown in Fig.4 indicate that SecFEC exceeds traditional simple free protocol.

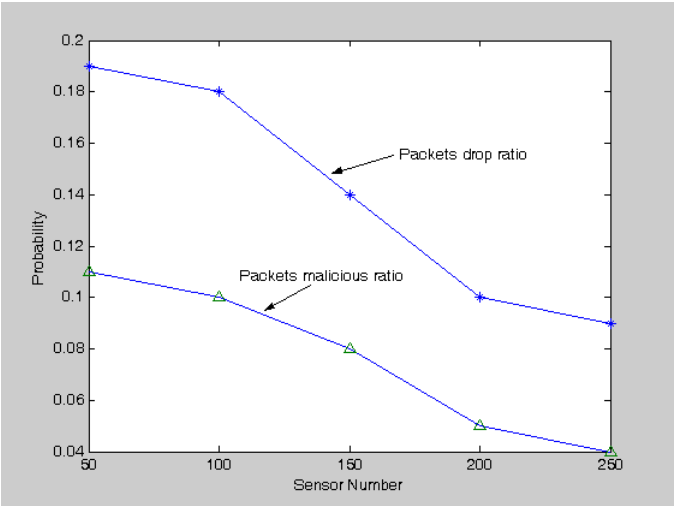

Fig. 4 Simulation Results

5. Conclusion

This paper proposed a secure and reliable multi-path transmission scheme named SRMR for UASN. The SRMR scheme has considered how to combine security transmission with reliability transmission together to improve network performance. In SRMR scheme, the sender sensor node uses secure forward error correction (SecFEC) erasure coding to encode each packet into multiple fragments and transmits the secure fragments to the sink over link-disjoint paths independently. The secure erasure coding using threshold secret sharing scheme allows the sink to reconstruct the original packet even if some of the fragments are lost or compromised. To our knowledge, design a secure and reliable compatible routing scheme for UASN is the first research in publish. Our future works are mobile secure.

6. Acknowledgment

This research is supported by the open foundation of Sonar Technology based National Defense Science and Technology Key Laboratory in 715th Research Institute of China Shipbuilding Industry Corporation**.**

7. References

[1] I. F. Akyildiz, D. Pompili, T. Melodia, “Underwater Acoustic Sensor Networks: Research Challenges.” Elsevier’s Journal of Ad Hoc Networks, 3(3), pp.257-279, 2005.

[2] L. Freitag, M. Stojanovicv, “Acoustic communications for regional undersea observatories.” Proceedings of Oceanology International, London, U. K., 2002.

[3] J. Heidemann, W. Ye, J. Wills, *et al*., “Research Challenges and Applications for Underwater Sensor Networking.” IEEE Wireless Communications and Networking Conference, Las Vegas, Nevada, USA, April 2006.

[4] I. F. Akyildiz, D. Pompili, T. Melodia, “Challenges for Efficient Communication in Underwater Acoustic Sensor Networks.” ACM SIGBED Review, Vol. 1, no. 1, July 2004.

[5] J. H. Cui, J. Kong, M. Gerla, *et al*., “Challenges: Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications.” Special Issue of IEEE Network on Wireless Sensor Networking, May 2006.

[6] Z. Ye, S. V. Krishnamurthy, S. K. Tripathi, “A Framework for Reliable Routing in Mobile Ad Hoc Networks.” IEEE INFOCOM 2003, 2003.

[7] C. Karlof, D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.” Ad Hoc Networks, 2003(1): 293-315.

[8] Wenjing Lou, Wei Liu, Yuguang Fang, “SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks.” IEEE INFOCOM 2004, Hong Kong, China, March 2004.

[9] H. Yih-Chun, A. Perrig, “A survey of secure wireless ad hoc routing.” IEEE Security & Privacy Magazine, 2(3): 28-39, May/June 2004.

[10] H. Yih-Chun, B. David, Johnson, et al., “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks.” Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY, June 2002.

[11] A. Nasipuri, S. R. Das, “On-Demand Multipath Routing for Mobile Ad Hoc Networks.” Proceedings of the 8th Int. Conf. on Computer Communications and Networks (IC3N), Boston, MA, 1999.

[12] S. Lee, M. Gerla, “Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks.” Proc. of IEEE ICC, Vol.10, May 2001: 3201-3205.

[13] Y. C. Hu, A. Perrig, D. B. Johnson, “Wormhole detection in wireless ad hoc networks.” Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[14] J. Deng, R. Hang, S. Mishra, “INSENS: Intrusion-Tolerant routing in wireless Sensor Networks.” Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, Nov 2002.

[15] C. Y. Wan, A. T. Campbell, “PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks.” Proc. ACM WSNA’02, Atlanta, GA, Sept. 28, 2002.

[16] Y. Sankarasubramaniam, O. B. Akan, I. F. Akyildiz, “ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks.” Proc. ACM Mobihoc’03, Annapolis, MD, June 1-3, 2003.

[17] G. G. Xie, J. Gibson, “A Networking Protocol for Underwater Acoustic Networks.” Technical Report TR-CS-00-02, Department of Computer Science, Naval Postgraduate School, December 2000.

[18] P. Xie, J. H. Cui, “SDRT: A Reliable Data Transport Protocol for Underwater Sensor Networks.” UCONN CSE Technical Report: UbiNet-TR06-03 (BECAT/CSE-TR-06-14), February 2006.

[19] R. Vasudevan, S. Sanyal, “A novel multipath approach to security in mobile ad hoc networks (MANETs) .” Proc. of Intl Conf. Computers and Devices for Communication (CODEC’04), Kolkata, India, Jan 2004.

[20] G. J. Simmons, “An Introduction to Shared Secret andior Shared Control Schemes and The Application.” Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992: 441-497.

[21] A. Shamir, “how to Share a Secrel.” Communications of the ACM, Nov 1979, 22(11): 612-613.

[22] J. Nonnenmacher, E. Biersack, J. Towsle, “Parity-Based Loss Recovery for Reliable Multicast Transmission.” SIGCOMM’97. Cannes, France, Sept 1997.

[23] J. C. HENRION, “An Efficient Software Implementation of a FEC Code.” Institute of Montefiore. University of Liege.1997.

[24] M. Stojanovia. On the relationship between capacity and sitance in an underwater acoustic communication channle. Proceedings of the 1st ACM international workshop on Underwater networks, volume 1, pages 41-47, 2006.