JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Delay Sensitive Energy Management Clusterhead Routing Protocol for Securing Underwater Acoustic Sensor Networks

S. Sahana[1*], V. Vinothini[2]

[1]Dept of CS, S.K.S.S College, Thiruppanandal, Tamilnadu
[2]Dept of CS, Idhaya College of Women, Kumbakonam, Tamilnadu

Corresponding Author: sahana2593@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**Underwater sensor network consists of number of various sensors and autonomous underwater vehicles deployed underwater to coordinate, interact and share information among them to carry out sensing and monitoring functions. Underwater environment differs from terrestrial radio environment both in terms of energy costs and channel propagation phenomena. The goal of the project is to reduce the occurrence of delays and attacks, during data transmission among sensor nodes in under water acoustic sensor network by introducing a protocol called delay sensitive energy management cluster head routing protocol in order to enhance the energy efficiency of the sensor network.

***Keywords*—** Underwater , Delays And Attacks , Sensor Network.

I. Introduction

The earth is a water planet, because more than 70% of its surface is covered by the sea and ocean, the remaining part are covered by human being. Several reasons attract to discover this underwater world such as the still large unexplored surface, the biological and geological wealth, the natural and man-made disasters, which have given rise to significant interest in monitoring oceanic environments for scientific, environmental, commercial, security and military fields [1]. Due to these reasons, underwater wireless sensor networks (UWSN) are very promising to this hostile environment. They have many potential applications, including ocean sampling networks, undersea explorations, disaster prevention, seismic monitoring, and assisted navigation [2]. The function of a routing protocol in UWSN is a fundamental part of the network infrastructure to establish routes between different nodes. UWSN routing protocols are difficult to design in general. It is a challenging task, caused by the aquatic environment. UWSN are significantly different from the terrestrial sensor technology. First, the suitable medium of communication inunderwater networks is the acoustic waves and is preferred to both radio and optical waves because they have great drawbacks in aquatic channel [3]. Secondly, the most terrestrial sensors are static, while underwater sensor nodes may be mobile with water movements and other underwater activities. Consequently the challenge imposed by UWSNs leads to the inability to adapt directly the existing routing protocols in terrestrial WSN, so new routing approach must be implemented for UWSN.

II. RELATED WORK

Y. Sankarasubramanian [4] describes the concept of sensor networks which has been made viable by the convergence of microelectro- mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored. Open research issues for the realization of sensor networks are also discussed. Cost function based routing has been widely studied in wireless sensor networks for energy efficiency improvement and network lifetime elongation.However, due to the complexity of the problem, existing solutions have various limitations. In this paper, we analyze the inherent factors, design principles and evaluation methods for cost function based routing algorithms. Two energy aware cost based routing algorithms named Exponential and Sine Cost Function based Route (ESCFR) and Double Cost Function based Route (DCFR) have been proposed in this paper. For ESCFR, its cost function can map small changes in nodal remaining energy to large changes in the function value. For DCFR, its cost function takes into consideration the end-to-end energy consumption, nodal remaining energy, resulting in a more balanced and efficient energy usage among nodes. The performance of the cost function design is analyzed. Extensive simulations demonstrate the proposed algorithms have significantly better performance than existing competing algorithms [5].

Compromised-node and denial-of-service are two key attacks in wireless sensor networks (WSNs). In this paper, we study routing mechanisms that circumvent (bypass) black holes formed by these attacks. We argue that existing multi-path routing approaches are vulnerable to such attacks, mainly due to their deterministic nature. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. In this paper, wedevelop mechanisms that generate randomized multipath routes. Under our design, the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy- efficient, making them quitecapable of bypassing black holes at low energy cost. Extensive simulations are conducted to verify the validity of our mechanisms [6].

Due to their limited capabilities, wireless sensor nodes are subject to physical attacks that are hard to defend against. In this paper, we first identify a typical attacker called parasitic adversary, who seeks to exploit sensor networks by obtaining measurements in an unauthorized way. As a countermeasure, we first employ a randomized key refreshing: with low communication cost, it aims at confining (but not eliminating) the effects of the adversary [7].

Moreover, our low-complexity solution, GossiCrypt, leverages on the large scale of sensor networks to protect data confidentiality, efficiently and effectively. GossiCrypt applies symmetric key encryption to data at their source nodes and re-encryption at a randomly chosen subset of nodes en route to the sink. The combination of randomized key refreshing and GossiCrypt protects data confidentiality with a probability of almost 1; we show this analytically and with simulations. In addition, the energy consumption of GossiCrypt is lower than a public- key based solution by several orders ofmagnitude.

As a prime target of the quality of privacy in vehicular ad hoc networks (VANETs), location privacy is imperative for VANETs to fully flourish. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. To cope with the issue, in this paper, we present an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy [8]. In particular, we first introduce the social spots where several vehicles may gather, e.g., a road intersection when the traffic light turns red or a free parkinglot near a shopping mall. By taking the anonymity set size as the location privacy metric, we then develop two anonymity set analytic models to quantitatively investigate the location privacy that is achieved by the PCS strategy. In addition, we use game- theoretic techniques to prove the feasibility of the PCS strategy in practice. Extensive performance evaluations are conducted to demonstrate that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots and that the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place.

III. PROPOSED WORK

In this paper, we will fill in this gap by optimizing watchdog techniques for WSNTSs to balance energy efficiency and security (in terms of trust accuracy and robustness). Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. To touch this goal, we optimize watchdog techniques in two level First,we optimize watchdog locations by considering the fact: although sensor nodes whichare located more closely may consume less energy to monitor each other due to shorter communication distance , these nodes are more likelyofbeing compromised together and launch collaborative attacks.We therefore explore theoptimal watchdoglocation (given a target node) to minimize the overall risk (in terms of both energy consumption and security). Second, we optimize watchdog frequency and reduce its redundancy.In particular, compared with the sensor nodes whose behaviours are more uncertain, the nodes with more determined trustworthiness (i.e., trustworthy or untrustworthy) may require less watchdog tasks (i.e., lower watchdog frequency) to further investigate. The Proposed System Architecture is shown below.

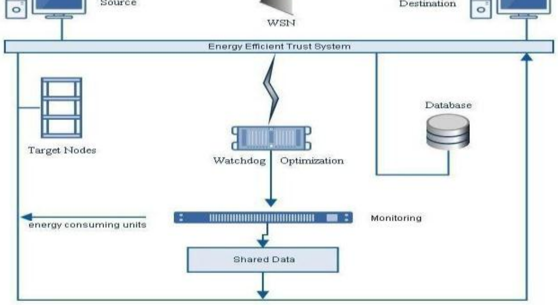

Fig 1 Proposed System Architecture

IV. METHODOLOGIES TRUSTSYSTEM

Client-server computing or networking is a distributed application that partitions watchdog‟s task between source and target nodes. Often clients and servers operate over a network on separate functionalities. A server machine is a high- performance host that is running one or more tasks which share its resources withnodes.

V. WATCHDOGS TECHNIQUE

All the active nodes in WSN, Once the correct destination router is found, an end-to-end peer connection (TCP or IP) is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use, permitting casual, any-to-any communication without the burden of specifying peer connections in advance. When performing watchdog tasks to monitor routing behavior, the watchdog nodes maywaste some watchdog tasks if they miss the target node‟s forwarding packets due to noises.

VI. TARGET NODES

The number of connections to establish between each pair of target node is established between each and every nodes for network communication. From the source node to the destination node and intermediates node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other. In multipath data transmission, send the data from source node that means which type of file size and fileextension.

VII. ENERGYCONSUMPTION

In proposed a energy-efficient trust model by applying a geographic target nodes to identify trust managers (may save energy due to low storage usage), while implemented an energy watcher to help sensor nodes estimate their neighbor nodes"energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route. Moreover, a watchdog‟s technology is widely used to estimate energy consumed by each task typicalfree space wireless radio model. In this model, asensor node‟s transmitter unit to the main node as file request and then the facts can be sends multiple requested node and DBP algorithms to avoid the WSNTS attacks. The source node sends all type of file, and then enters the data sends from source node to destination node over the network. As well as data must be send from source node to intermediate node automatically in this module the data‟s are successfully transfer from source to destination withoutattacks.

VIII. CONCLUSION

UW-MAC, a distributed MAC protocol forunderwater acoustic sensor networks, was proposed. It is a transmitter-based CDMA scheme that incorporates a closed-loop distributed algorithm to set the optimal transmits power and code length. It is proven that UW-MAC manages to simultaneously achieve high network throughput, limited channel access delay, and low energy consumption in deep water communications, which are not severely affected by multipath. In shallow water communications, which are heavily affected by multipath, UW-MAC dynamically finds the optimal trade-off among these objectives.

REFERENCES

[1]. Manjula, R.B. and Sunilkumar, S. M. (2011)Issues in Underwater Acoustic Sensor Networks", International Journalof Computer and Electrical Engineering, Vol.3, No.1, pp.101-110.

[2]. Akyildiz, I. F., Pompili,D., Melodia, T.(2006) State of the Art in Protocol Research for Underwater Acoustic Sensor Networks,The First ACM International Workshop on UnderWater Networks (WUWNet06) 2006, Los Angeles, California, USA,pp.7-17.

[3]. Liu, L., Zhou, S., and Cui, J. H., (2008)

[4]. “Prospects and Problems of Wireless Communication for Underwater Sensor Networks”, WILEY WCMC, Vol. 8, Pages977-994.

[5]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393–422,Mar. 2002.

[6]. A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, “Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks,” Computer Networks, vol. 56, no. 7, pp. 1951–1967, May.2012.

[7]. T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sen- sor networks using randomized dispersive routes,” IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp.941–954,

[8]. Jul. 2010.

[9]. P. Papadimitratos, J. Luo, and J. P. Hubaux, “A randomized coun-termeasure against parasitic adversaries in wireless sensor networks,” IEEE Journal on Selected Areas in Communications, vol. 28, no. 7, pp. 1036–1045, Sep.2010.