ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Swarm Intelligence Based Warmhole Detection Technique For Under Water Sensor Networks

S.Venkatramulu, Dr.C.V.Guru rao

Assoc. Prof. Department of CSE, K.I.T.S Warangal, A.P, India

Professor & Principal, Department of CSE, S.R Engineering College Warangal, A.P, India

ABSTRACT: In aquatic applications, Underwater Sensor Network (UWSN) has emerged as a powerful technique. Features of UWNS are long propagation, low bandwidth and high error rate. Existing protocol or algorithm design for terrestrial network to UWNS becomes quite difficult to apply due to limited power capacity and node mobility. At every layer of the stack protocol, it requires a new research and there is a need of general architecture in UWSN. Underwater wireless sensor network consists of a certain number of sensors which sends the sensed data to the sink node and performs a collaborative task. In favor of wireless transmission, UWSN frequently chooses acoustic as a communication medium. Shallow water has a great value in undergoing special environment offered by UWSN. Mobility of sensor node due to water current, delay and loss in propagation are significant aspect of terrestrial sensor network. In UWSN, information is delivered from sensor nodes to sink node that possess an innovative challenge in underwater sensor network, warm hole attack causes serious issue in sensor networks. Defending against wormhole attack is a challenging task, there is no mechanism evolved for wormhole detection in under water sensor networks. We propose to develop a warm hole detection technique based on swam intelligence.

KEYWORDS: aquatic application; underwater sensor network; node mobility; wormhole attack; sensor nodes.

I. INTRODUCTION

Wireless ad hoc and sensor networks have gained popularity in recent years for the ease of deployment due to their infrastructure-less nature. One obvious use of such networks is in hostile environments for communications, monitoring, sensing etc. But being a broadcast medium, wireless medium offers an innate advantage to any adversary who intends to spy in or disrupt the network. Wormhole attacks are one of most easy to deploy for such an adversary and can cause great damage to the network. **Wormhole Attack:** For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the ***wormhole link***. The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the Wormhole link and replays them at the end.

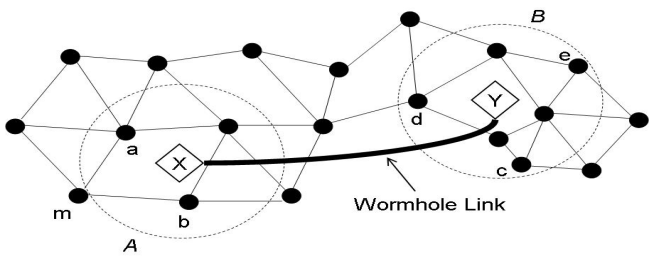

Fig.1.wireless sensor network with wormhole attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

An example is shown in the above figure Fig.1, Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

Underwater acoustic communication is a technique of sending and receiving message below water. There are several ways of employing such communication but the most common is using hydrophones. Under water communication is difficult due to factors like multi-path propagation, time variations of the channel, small available bandwidth and strong signal attenuation, especially over long ranges. In underwater communication there are low data rates compared to terrestrial communication, since underwater communication uses acoustic waves instead of electromagnetic waves.

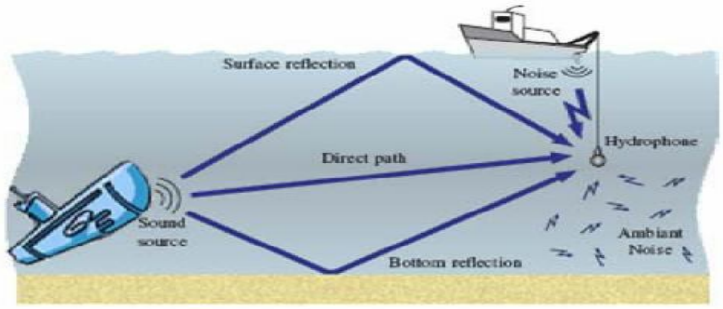

Fig.2.underwater sensor network.

Example of multi-path propagation there are four different types of nodes in under water sensor network system shown in Fig.2. The large number of sensor nodes is deployed on or near to the sea floor at the lowest layer. Storage capacity, power computing and price are moderate. They spent most of their life asleep in long-term operation and batteries in sensor collects the data. Internet connection can connect and control more than one node at the top layer. These controls are situated with power on the off-shore or on-shore. These nodes have a larger storage capacity to buffer the data. Sensor nodes directly communicate with the control node through a relay node. In large network, super node is a third type of node which can access high speed network. It permits richer network connectivity [2].Swarm intelligence (SI) is the collective behavior of decentralized, self-organized systems, natural or artificial. The concept is employed in work on artificial intelligence. The expression was introduced by Gerardo Beni and Jing Wang in 1989, in the context of cellular robotic systems.SI systems consist typically of a population of simple agents interacting locally with one another and with their environment. The inspiration often comes from nature, especially biological systems. The agents follow very simple rules, and although there is no centralized control structure dictating how individual agents should behave, local, and to a certain degree random, interactions between such agents lead to the emergence of "intelligent" global behavior, unknown to the individual agents. Examples in natural systems of SI include ant colonies, bird flocking, animal herding, bacterial growth, and fish schooling. The definition of swarm intelligence is still not quite clear. In principle, it should be a multi-agent system that has self-organized behavior that shows some intelligent behavior. The application of swarm principles to robots is called swarm robotics, while 'swarm intelligence' refers to the more general set of algorithms. 'Swarm prediction' has been used in the context of forecasting problems. Many swam

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

intelligent algorithms are there one of the algorithm is ant colony optimization algorithms this is used in our proposed method.

A. Application Of Under Water Sensor Networks:

We see our approaches as applicable to a number of applications, including seismic monitoring, equipment monitoring and leak detection, and support for swarm's underwater robots. We review the different characteristics of each of these below.

Ocean Sampling Networks. Networks of sensors and AUVs, such as the Odyssey-class AUVs, can perform synoptic, cooperative adaptive sampling of the 3D coastal ocean environment.[3]

Distributed Tactical Surveillance. AUVs and fixed underwater sensors can collaboratively monitor areas for surveillance, reconnaissance, targeting and intrusion detection systems. [4]

Seismic monitoring: A promising application for underwater sensor networks is seismic monitoring for oil extraction from underwater fields. Frequent seismic monitoring is of importance in oil extraction; studies of variation in the reservoir over time are called .4-D seismic and are useful for judging fields performance and motivating intervention. [4]

Equipment Monitoring and Control: Underwater equipment monitoring is a second example application. Ideally, underwater equipment will include monitoring support when it is deployed, possibly associated with power and communications. Short-term equipment monitoring shares many technical requirements of long-term seismic monitoring, including the need for wireless (acoustic) communication, automatic configuration into a multi-hop network, localization (and hence time synchronization), and energy efficient operation[4]

Flocks of Underwater Robots: A third and very different application is supporting groups of underwater autonomous robots. Applications include coordinating adaptive sensing of chemical leaks or biological phenomena (for example, oil leaks or phytoplankton concentrations), and also equipment monitoring applications as described above. Communication for coordinated action is essential when operating groups of robots on land. Underwater robots today are typically either fully autonomous but largely unable to communicate and coordinate with each other during operations, and therefore able to communicate, but limited in deployment depth and maneuverability [4].

B. Challenges Of UWSN:

- The available bandwidth is severely limited The underwater channel is severely impaired, especially due to multi- path and fading problems;
- Propagation delay in underwater is five orders of magnitude higher than in radio frequency (RF) terrestrial channels, and extremely variable;
- High bit error rates and temporary losses of connectivity (shadow zones) can be experienced, due to the extreme characteristics of the underwater channel;
- Battery power is limited and usually batteries cannot be recharged, also because solar energy cannot be exploited;
- Underwater sensors are prone to failures because of fouling and corrosion.
- Ground-based sensor network or UAN techniques cannot meet a wide variety of aquatic application demands to implement a localized, precise, and large-scale sensing technology in aquatic environments. Due to the complexity of the aquatic environments and the sophistication of the user scenarios, designing a distributed and scalable UWSN is a very challenging task.[6]
- The system lifetime of an underwater sensor network may vary from several minutes to several years. Such Heterogeneous system requirements are challenging underwater sensor network designs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

C. Security Issues Of UWSN:

Security is a broadly used term encompassing the characteristics of authentication, Confidentiality, integrity, data freshness, privacy, non repudiation, and anti-playback. Authentication, integrity privacy, non-reputation and anti-playback are some of the characteristic of security.

- A critical security issue is to defend against denial-of-service attack which could be in the form of (1) depleting node's on device resource (especially draining battery by incurring extra computation and communication) and (2) disrupting network collaboration (e.g., routing, data aggregation, localization, clock synchronization). Such attacks can disrupt or even disable ad hoc networks and sensor networks independent of cryptographic protections.[5]
- Security threat is a cross layer issue that affects the entire protocol stack. A self-organizing ad hoc network needs more protections than cryptography. We have extensively studied *low-cost underwater denial-of-service attacks* . The result is disastrous for multi-hop packet delivery. Distributed localization, and time-synchronization. desires more protections than cryptography
- To realize a scalable ad hoc network, nodes must be low-cost and economically viable. They are limited in energy, computation, and communication capabilities. This makes many existing security mechanisms inadequate, and hence inspires new security research, such as efficient key management authentication data privacy and anonymity that avoids expensive Denial crypto-operations. Security attacks continue to threaten ad hoc networks even when an ideal cryptosystem is efficiently protecting the network. A critical security issue is to defend against denial-of-service attack, which could be in the form of depleting node's on-device resource (especially draining battery by incurring extra computation and communication) and disrupting network collaboration (e.g., routing, data aggregation, localization, clock synchronization).

II. RELATED WORK

A. Visualization of wormholes in underwater sensor network:

Distributed visualization of wormhole, without depending on any hardware protects against wormhole in under water sensor network (UWSN). By measuring the propagation delay of acoustic signal, using multi-dimensional scaling every single sensor modernizes the local network topology. Hence the visualizing the deformation in edge length and angles in abut sensor the wormhole can be detected by Dis-Vow. Based on the distortions of an edge length and angles a normalized variable wormhole indicator is distinct so as to identify the fake neighboring connection. The simulation this paper evaluates the detection accuracy. Without introducing false positive alarm at most all the fake neighboring connections are detected by Dis-Vow. The intrigue establishes a limited amount of computation and storage overhead the sensors. The false positive alarm is reduced by using security Dis-Vow method. Then the frequency to accomplish wormhole detection is viewed in this paper. Dis-Vow extension is underneath erection. Plan can be pertained in a distributed detection mechanism to land based sensor network in 3D environment and multiple wormholes on localized network also modernized in this paper. Hence this research leads to a more accurate, robust and efficient solution to defend against wormhole attacks. [10]

B. Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes:

In [12], Using of beacon nodes in the detection and locating of wormhole attack was a challenging one to deal since the opponent does not need to negotiate any node. In order to send the packets of low latency channel, laptop or other wireless devices are used. Beacon nodes are implicit to discern their coordinates, between each pairs of nodes the straight line distance is calculated and compared by means of corresponding hop distance such as hop counts x node's transmission range R. Thus it is an easy and efficient method to detect and locate wormhole. Based on the information the auxiliary steps can be made so as to find the approximate location of the wormhole.

C. Dawwsen: A Defense Mechanism against Wormhole Attack in Wireless Sensor Network:

In [13], designing of DAWWSEN is done in which proactive routing protocol is based on the erection of hierarchical tree where base station is the root node, and sensor are the leaf or internal node of the tree. The base station disseminate the request packet in turn discovers the children node in which the tree construction is instigated by the base station. Node ID's are present in a request packet. The Id of the request packet and hop count should be identical in the instance of request packet sent by the base station. The parent can be determined as soon as the first request packet is sent, so they have to wait for certain interval of time so as to collect a number of request packet. It is still unfeasible to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

discern if the received request packet is reiterated by the wormhole or not. So as to over come this problem "time checker" and "request time" are a new entries which is been inserted by each nodes that receives the request packet. Prior to the retransmission and constructing of the request packet the base station waits for the Trefresh. In future some modification can be made in a routing protocol so as to get the balanced tree where the loads are reasonably distributed node since it reduces the value of Trefresh.

D. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks:

In industries, health care, public-safety and military environment wireless networks are enhanced to a greater extend. Security is tremendously significant in this situation. The preventative and detective measures are required to secure a wireless network. In [14], three mechanisms are adopted to modify the wireless MAC protocol. They are Positive acknowledge, detection strategy and MAC layer changes. The presence of adversary conducting a frame-relaying attack (such as man-in-the-middle and wormhole attack) can be highlighted by wireless MAC protocol. Problems for effective frame relaying attack are presented by Positive acknowledgment. Both the sender and receiver agree certain frame-relay attack, confess the reasonable station remain still at the time of detection tactic. Changes in the MAC layer can broaden the procedure that is reliable for sending encrypted, unicast and data frames [14].

III. PROPOSED SOLUTION

Wormhole attack causes serious issues in sensor networks. On the other hand defending against wormhole attack is a challenging task. To the best our knowledge, there is no mechanism evolved for wormhole detection in under water sensor networks.In [13], He Ronghui et al. have proposed an efficient method to detect and locate wormholes. They have proposed that method for wireless sensor networks. Further, they have used probe messages and alarm messages to detect and locate wormhole attackers, which increase control overhead. In addition to these, the gathered hop count and hop distance values are not secured using any security mechanism.In this proposal, we enhance the method introduced in [13] and amend with swarm intelligence, so that it will be suitable for underwater sensor networks.Swarm intelligence is the emergent collective intelligence of groups of simple autonomous agents. Here, an autonomous agent is a subsystem that interacts with its environment, which probably consists of other agents, but acts relatively independently from all other agents. [15].

The Ant colony optimization is based on the foraging behavior of ants. When ants search for food, they wander randomly and upon finding food return to their colony while laying a chemical substance called pheromone. Many ants may travel through different routes to the same food source. The ants, which travel the shortest path, reinforce the path with more pheromone that aids other ants to follow. [16].A large part of the research in swarm intelligence has focused on the reverse engineering and the adaptation of collective behaviors observed in natural systems with the aim of designing effective algorithms for distributed optimization. These algorithms, like their natural systems of inspiration, show the desirable properties of being adaptive, scalable, and robust. these are key properties in the context of network routing, and in particular of routing in wireless sensor networks .therefore, in the last decade ,a number of routing protocols for wireless sensor networks have been developed according to the principles of swarm intelligence ,and in particular ,taking inspiration from the forging behaviors of ant and bee colonies. Our proposed architecture encompass of base station, set of sensor nodes and set of anchor nodes. Nodes that are aware of their absolute location are marked as anchor nodes and nodes that are unaware of their locations are simply sensor nodes. Anchor nodes which know their geographic positions and non anchor nodes which do not know their positions.

The shortest distance between two anchor nodes are estimated using swarm intelligence routing algorithm. Each node periodically sends forward ants and gathers distance information between two anchor nodes. The backward ant updates the table by traversing in the reverse path. Then the actual distance between the anchors nodes are estimated using the RSS and transmission range measurements. Actual distance and estimated distance should be same. If there is a deviation, which is greater than a minimum threshold, then it is assumed that there is a presence of wormhole attack. Once we discover there is a fake neighboring connection, the detection mechanism will be activated to locate the ends of the wormhole and detect it by using false positive alarm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

During the distance estimation procedures, the distance information must be protected by shared secret keys between the anchors to prevent a malicious node from impersonating remote peers and gives authentication between each anchor nodes.After detecting the wormhole attacker, the anchors will broadcast the identity of the detected node to other nodes so that further communication from that node will be blocked.

A. Merits of Our Proposed Method:

- Our technique is the first approach that detects wormhole attacker in under water sensor network.
- By using swarm intelligence, our approach detects the worm hole attacker accurately.
- This method not only detects the wormhole attacker but also estimates the location of wormhole link and points.
- This approach secures the distance information of the anchor nodes using shared secret keys.

IV. CONCLUSION

Underwater wireless sensor network consists of a certain number of sensors which sends the sensed data to the sink node and performs a collaborative task. In favor of wireless transmission, UWSN frequently chooses acoustic as a communication medium. Many attacks are there in under water sensor networks, Warm hole attack causes serious issue in sensor networks. Defending against warm hole attack is a challenging task. We propose to develop a warm hole detection technique efficiently and effectively based on swam intelligence Algorithm.

REFERENCES

1. John Heidemann, Milica Stojanovic, and Michele Zorzi, "Underwater Sensor Networks: Applications, Advances, and Challenges". Philosophical Transactions of the Royal Society-A, p. accepted to appear, 2011
2. Wei Ye, John Heidemann, syed A, yunan Li, "Underwater Sensor Networking: Research Challenges and Potential Applications", IEEE Wireless Communications and Networking Conference (WCNC), pp- 228 – 235, 2006.
3. Haiming Yang; Sikdar, B, "A Mobility Based Architecture for Underwater Acoustic Sensor Network", EEEGlobalTelecommunicationsConference (GLOBECOM), pp- 1 – 5, 2008.
4. Ahmed M Mahdy, "Research Challenges and Applications for Underwater Sensor Network", IEEE Marine Wireless Sensor Networks: Challenges and Applications, Seventh International Conference on Networking (ICN) 2008 (2008)
5. Manjula.R.B, Sunilkumar S. Manvi, "Issues in Underwater Acoustic Sensor Networks", IEEE International Journal of Computer and Electrical Engineering (IJCEE), Vol-3, No-1, 2011.
6. Sasikanth Avancha, Anupam Joshi, and John Pinkston, "Security for Sensor Networks**",** Wireless Sensor Networks (WSN), pp -253-275, January 01, 2004
7. J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in Proc. of 2002 CADIP, Research Symposium (CADIP'02), Baltimore, USA, October 2002.
8. E.A. Basha, S. Ravela, and D. Rus, "Model-based monitoring for early warning flood detection", In Proc. SenSys, 2008, pp 295-308.
9. Dario Pompili, Tommaso Melodia, Ian F. Akyildiz, "A CDMA-Based Medium Access Control for Underwater Acoustic Sensor Networks", IEEE Transaction on Wireless Communication, Vol 8, No- 4, April 2009.
10. W.Wang, J.Kong, B.Bhargava and M.Gerla, "Visualization of Wormholes in underwater Sensor Network", International Journal of Security and Networks (IJSN), Volume 3, No.1, pp 10-23, 2008.
11. J. kong, Z. Ji , W. Wang, R. Bhargava, M. Gerla and R.Bagrodia, "Low-cost Attack against Packet Delivery, Localization and Time Synchronization Service in Under-water Sensor Network", In fourth ACM Workshop on Wireless Security (WiSe), 2005.
12. Y.-C. Hu, A. Perrig, and D. B.Johnson. Packet Leashes, "A Defense against Wormhole Attacks in Wireless Networks", in proceedings of IEEE INFOCOM, 2003
13. He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan, "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", WASE International Conference on Information Engineering, pp 251-254, 2009
14. Glass, S.M, Muthukkumarasamy V, Portmann. M, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks", IEEE Advanced Information Networking and Applications, pp -530 – 538, 2009.
15. Saleem, M.Di.Caro, G. Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions", Information Science, 2010.
16. Vasundhara Uchhula and Brijesh Bhatt, "Comparison of different Ant Colony Based Routing Algorithms", International Journal of Computer Applications, pp-97–101, 2010.
17. M. Heissenbüttel and T. Braun, "Ants-Based Routing in Large Scale Mobile Ad-Hoc Networks", http://www.iam.unibe.ch/~heissen/Papers/KIVS03_Final.pdf, 2003.