ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Securing Underwater Wireless Communication Networks

Ekta Deshmukh[1], Rajendra Singh Yadav[2], Nandini Upadhyay[3]

Research Scholar, Dept of Electronics and Communication, Gyan Ganga College of Technology, Jabalpur, India[1, 3]

Asst. Professor, Department of Electronics and Communication, Gyan Ganga College of Technology, Jabalpur, India[2]

Abstract: Underwater wireless communication networks are particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. The unique characteristics of the underwater acoustic communication channel and the differences between underwater sensor networks and their ground-based counterparts require the development of efficient and reliable security mechanisms. In this seminar, a complete survey of security for UWCNs is presented, and the research challenge for secure communication in this environment is outlined.

Keywords: Underwater wireless communication networks ground-based counterparts require the development

I. INTRODUCTION

Underwater wireless communication networks (UWCNs) are constituted by sensors and autonomous underwater vehicles (AUVs) that interact to perform specific applications such as underwater monitoring. Coordination and sharing of information between sensors and AUVs make the provision of security challenging. The aquatic environment is particularly unreliable to malicious attacks due to the high bit error rates, large and variable. propagation delays, and low bandwidth of acoustic channels.

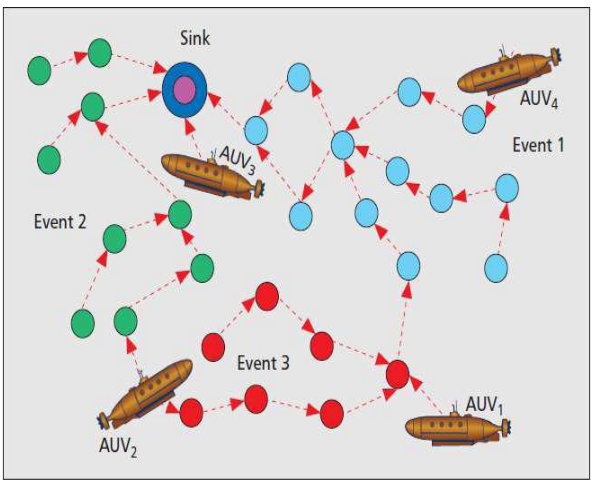

Fig.1 Underwater sensor network with AUV

Achieve in reliable inter vehicle and sensor-AUV communication is especially difficult due to the mobility of AUVs and the movement of sensors with water currents The unique characteristics of the underwater acoustic channel ,and the differences between underwater sensor networks and their ground based counterparts require the development of efficient and reliable security mechanisms. then the single best solution for communicating underwater ,lower frequency 10hz lesser then that it's not possible to propagation of sound ,higher frequency 1mhz above are rarely used because they are absorbed very quickly and then buoy is one of the important hardware in my project.

II. ATTACKS ON UWCNS ANDCOUNTERMEASURESJAMMIN

A jamming attack consists of interfering with the physical channel by putting up carriers on the frequencies neighbor nodes use to communicate. Since underwater acoustic frequency bands are narrow, UWCNs are vulnerable to narrowband jamming. Localization is affected by the replay attack when the attacker jams the communication between a sender and a receiver, and later replays the same message with stale information posing as the sender.

Spread spectrum is the most common defense against jamming. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) in underwater communications are drawing attention for their good performance under noise and multipath interference. These schemes are resistant to interference from attackers, although not infallible. An attacker can jam a wide band of the spectrum or follow the precise hopping sequence when an FHSS scheme is used. A high-power wideband jamming signal can be used to attack a DSSS scheme. Underwater sensors under a jamming attack should try to

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

preserve their power. When jamming is continuous, sensors can switch to sleep mode and wake up periodically to check if the attack is over. When jamming is intermittent, sensors can buffer data packets and only send high-power high priority messages to report the attack when a gap in jamming occurs. In ground-based sensor networks, other sensors located along the edge of the area under normal background noise and report intrusion to outside nodes. That will cause any further traffic to be rerouted around the jammed region. However, this solution cannot be applied to UWCNs, since nodes underwater are usually sparsely deployed, which means there would not be enough sensors to delimit the jammed region accurately and reroute traffic around it.

A. Wormhole Attack:

A wormhole is an out-of-band connection created by the adversary between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. This connection uses fast radio (above the sea surface) or wired links to significantly decrease the propagation delay.

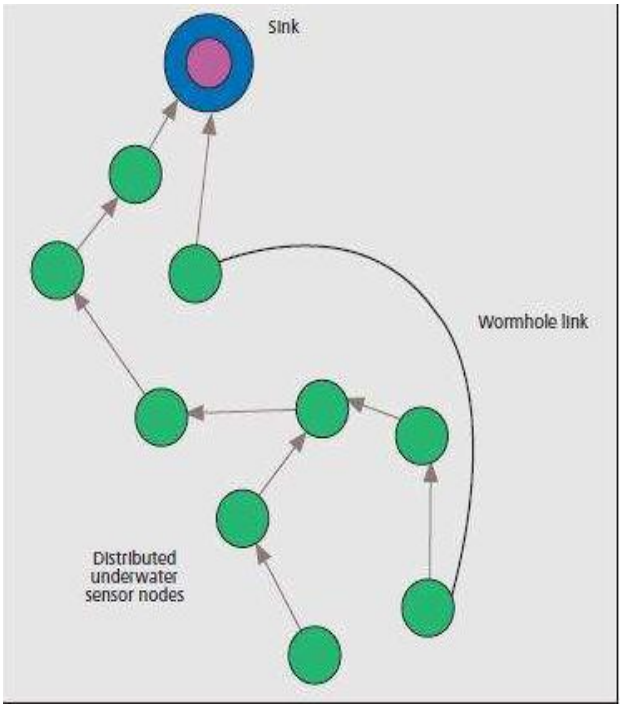

Fig. Underwater network with a wormhole link

In a wormhole attack the malicious node transfers some selected packets received at one end of the wormhole to the other end using the out-of-band connection, and re-injects them into the network. The effect is that false neighbor relationships are created, because two nodes out of each other's range can erroneously conclude that they are in proximity of one another due to the wormhole's presence. This attack is devastating. Routing protocols choose routes that contain wormhole links because they appear to be shorter; thus, the adversary can monitor network traffic and delay or drop packets sent through the wormhole. Localization protocols can also be affected by these attacks when malicious nodes claim wrong locations and mislead other nodes.

One proposed method for wormhole detection in ground-based sensor networks consists of estimating the real physical distance between two nodes to check their neighbor relationship. If the measured distance is longer than the nodes' communication range, it is assumed that the nodes are connected through a wormhole. However, accurate distance estimation depends on precise localization (geographical packet leashes, wormhole detection using position information of anchors), tight clock synchronization (temporal packet leashes), or use of specific hardware (directional antennas).

B. Sybil Attack:

An attacker with multiple identities can pretend to be in many places at once. Geographic routing protocols are also misled because an adversary with multiple identities can claim to be in multiple places at once Authentication and position verification are methods against this attack, although position verification in UWCNs is problematic due to mobility.

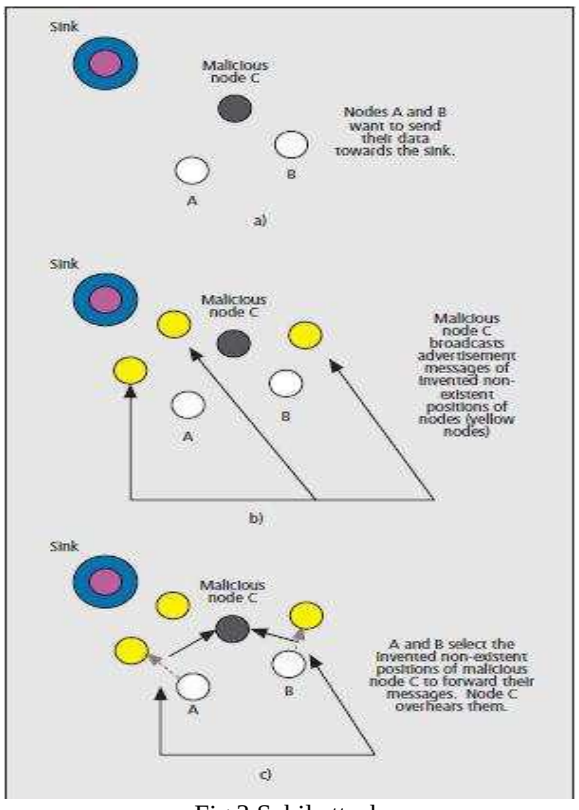

Fig.3 Sybil attack

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

C. Sinkhole Attack:
In a sinkhole attack, a malicious node attempts to attract traffic from a particular area toward it; for example, the malicious node can announce a high-quality route. Geographic routing and authentication of nodes exchanging routing information are possible defenses against this attack, but geographic routing is still an open research topic in UWCNs.

D. Hello Flood Attack:
A node receiving a HELLO packet from a malicious node may interpret that the adversary is a neighbor; this assumption is false if the adversary uses high power for transmission. Bidirectional link verification can help protect against this attack, although it is not accurate due to node mobility and the high propagation delays of UWCNs. Authentication is also a possible defense.

Acknowledgment Spoofing:
A malicious node overhearing packets sent to neighbor nodes cause this information to spoof link layer acknowledgments with the objective of forcing a weak link or a link located in a shadow zone. Shadow zones are formed when the acoustic rays are bent and sound waves cannot penetrate. They cause high bit error rates and loss of connectivity. This way, the routing scheme manipulated. A solution to this attack would be encryption of all packets sent trough the network.

III. SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered:

1. Authentication:
Authentication is the proof that the data was sent by a legitimate sender. It is essential in military and safety-critical applications of UWCNs. Authentication and key establishment are strongly related because once two or more entities verify each other's authenticity, they can establish one or more secret keys over the open acoustic channel to exchange information securely; conversely, an already established key can be used to perform authentication. Traditional solutions for key generation and update (renewal) algorithms should be adapted to better address the characteristics of the underwater channel. A key generation system is proposed that requires only a threshold detector, lightweight computation, and communication costs.

2. Confidentiality:
Confidentiality means that information is not accessible to unauthorized third parties. Therefore, confidentiality in critical applications such as maritime surveillance should be guaranteed.

3. Integrity:
It ensures that information has not been altered by any adversary. Many underwater sensor applications for environmental preservation, such as water quality monitoring, rely on the integrity of information.

4. Availability:
The data should be available when needed by an authorized user. Lack of availability due to denial-of-service attacks would especially affect time-critical aquatic exploration applications such as prediction of seaquakes.

IV. RESEARCH CHALLENGES

The security issues and open challenges for secure time synchronization, localization, and routing in UWCNs are summarized in the following sections:
Secure Time Synchronization:
Time synchronization is essential in many underwater applications such as coordinated sensing tasks. Also, scheduling algorithms such as time division multiple access (TDMA) require precise timing between nodes to adjust their sleep-wake up schedules for power saving. Achieving precise time synchronization is especially difficult in underwater environments due to the characteristics of UWCNs. For this reason, the time synchronization mechanisms proposed for ground-based sensor networks cannot be applied, and new mechanisms have been proposed. Tri-Message is a time synchronization protocol designed for high-latency networks with a synchronization precision that increases with distance. A multilateration algorithm is proposed in for localization and synchronization in 3D underwater caustic sensor networks. It is assumed that a set of anchors, several buoys on the ocean surface, already know their locations and time without error.
The following open research issues for secure time synchronization need to be addressed:

• Because of the high and variable propagation delays of UWCNs, the time required to synchronize nodes should be investigated.
• Efficient and secure time synchronization schemes with small computation and communications costs need to be designed to defend against delay and wormhole attacks.

V. SECURE LOCALIZATION

Localization is a very important issue for data tagging. Sensor tasks such as reporting the occurrence of an event or monitoring require localization information. Localization can also help in making routing decisions. For example, the underwater sensors in learn the location and speed of mobile beacons and neighbors during the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

localization phase; the position and motion of mobile beacons are used by the routing protocol to choose the best relay for anode to forward its data.

Localization approaches proposed for ground-based sensor networks do not work well underwater because long propagation delays, Doppler Effect, multipath, and fading cause variations in the acoustic channel. Band width limitations, node mobility, and sparse deployment of underwater nodes also affect localization estimation. Localization schemes can be classified into:

- Range-Based Schemes
- Range-Free Schemes

A. RANGE-BASED SCHEMES (using range and/or bearing information):

The location of nodes in the network is estimated through precise distance or angle measurements.

Advantages And Disadvantages:

Range-based localization method can provide more accurate position estimation. They need additional hardware for distance measurement, which leads to the increase in the network cost correspondingly. Relatively, range-free schemes do not need additional hardware support. However, range-free schemes can only provide coarse position estimations. Localization algorithms also can be classified into distributed and centralized. In distributed algorithms, each unknown node plays a part in localization information collection and runs a distance estimation algorithm individually. On the contrary, in centralized localization algorithms, a central unit is responsible for estimating the location of each unknown node, which will be bound to increase the burden of the central unit and reduce the lifetime of the whole networks. Experiments show that distributed localization protocols are more effective for large-scale UASNs.[7]

Anchor-Based Schemes:

Anchor nodes are deployed at the seabed or sea surface at locations determined by GPS. The propagation delay of sound signals between the sensor or AUV and the anchors is used to compute the distance to multiple anchor nodes.

Advantages:

After finding the subset (anchor nodes), we tackle the problem of localizing the chosen nodes. To localize the anchor nodes, we resort – as previously mentioned – to regarding anchor nodes as nodes that are capable of communicating with surface buoys and localizing themselves. We assume this property for all deployed nodes since the subset of anchor nodes is determined after deployment and thus no nodes are “special”. Using existing underwater GPS systems, such as GIB [3], the anchor nodes with their ability to communicate with several surface buoys can localize themselves. Obviously, due to the complexity and energy consumption of GIB, it cannot be used on all the deployed nodes leading to our proposed research work.

Distributed Positioning Schemes:

Positioning infrastructure is not available, and nodes communicate only with one-hop neighbors and compute their locations using multilateration. Underwater sensor positioning (USP) has been proposed in as a distributed localization scheme for sparse 3D networks, transforming the 3Dunderwater positioning problem into a2D problem using a distributed non degenerative projection technique. Using sensor depth information, the neighboring reference nodes are mapped to the horizontal plane containing the sensor to be localized. After projecting the reference nodes, localization methods for 2D networks such as bilateration or trilateration can be used to locate the sensor.

Advantages:

used UWSN localization with 3D architecture may be more tricky than with 2D architecture. In 2D architectures, the sensing coverage will be only in a particular plane, thereby restricting itself to scan only the plane covered by the nodes.

.Every node in an UWSN communicates using acoustic signals. These signals experience propagation delay because of the ocean parameters like Pressure, Temperature, Salinity and Altitude. While devising an efficient localization algorithm it becomes very crucial to study the impact of above parameters on the algorithm.

In 3D UWSN, out of the three coordinates (x,y,z), one of the coordinate i.e. depth can be found by a pressure sensor. Finding the Depth of a node becomes much easier by using pressure sensors. But at the same time we cannot neglect the errors encountered during depth calculation.[8]

Schemes That Use Mobile Beacons/Anchors:

They use mobile beacons whose locations are always known. Scalable localization with mobility prediction (SLMP) has been proposed in as arc hierarchical localization scheme. At the beginning, only surface nodes know their locations, and anchor nodes can be localized by these surface buoys. Anchor nodes are selected as reference nodes because of their known locations; with the advance of the location process more ordinary nodes are localized and become reference nodes. During this process, every node predicts its future mobility pattern according to its past known location information.

B. RANGE-FREE SCHEMES (Not Using Range Or Bearing Information):

They have been designed as simple schemes to compute only coarse position estimates. A range-free scheme estimates the location of a sensor within a certain area. None of the aforementioned localization schemes was

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

designed with security in mind. Some localization-specific attacks (replay attack, Sybil attack, worm hole attack) have previously been described.

Open research issues for secure localization are:

• Effective cryptographic primitives against injecting false localization information in UWCNs need to be developed.

• It is necessary to design resilient algorithms able to determine the location of sensors even in the presence of Sybil and wormhole attacks.

• Techniques to identify malicious or compromised anchor nodes and to avoid false detection of these nodes are required.

• Secure localization mechanisms able to handle node mobility in UWCNs need to be devised.

TABLE: BASIC COMPARISON BETWEEN RANGE BASED AND RANGE FREE SCHEME

RANGE FREE	RANGE BASED
They No need additional hardware for distance measurement	They need additional hardware for distance measurement
It is large scale under water wireless communication	In this scheme range is predefined in under water wireless communication.
Effective cryptographic primitives against injecting false localization information in UWCNs need to be developed	This is not available in this scheme.
It is necessary to design resilient algorithms able to determine the location of sensors even in the presence of Sybil and wormhole attacks.	In this scheme this featured not Available.
Techniques to identify malicious or compromised anchor nodes and to avoid false detection of these nodes are required.	Techniques are not identify malicious or compromised anchor nodes and to avoid false detection of these nodes are required.

VI. SECURE ROUTING

Routing is essential for packet delivery in UWCNs. For example, the Distributed Underwater Clustering Scheme (DUCS) does not use flooding and minimizes the proactive routing message exchange. Routing is specially challenging in UWCNs due to the large propagation delays, the low bandwidth, the difficulties of battery refills of underwater sensors, and the dynamic topologies. Therefore, routing protocol should be designed to be energy-aware, robust, scalable and adaptive. Many routing protocols have been proposed for underwater wireless sensor network .However, none of them has been designed with security as a goal. Routing attacks can disable the entire network's operation. Spoofing, altering, or replaying routing information affects routing.

VII. CONCLUSIONS

This paper gives the overall view of the necessity of underwater wireless communication and its applications. Despite much development in this area of the underwater wireless communication, there is still an immense scope so more research as major part of the ocean bottom yet remains unexploded. Underwater Sensor Networks is a very recent technology that tries to follow the same steps than terrestrial wireless networks in a very different and challenging network environment. There is an increasing interest in USWN technologies and their potential applications. Underlining the specific characteristics of these networks, possible attacks, and counter measures. The main research challenges related to secure time synchronization, localization, and routing have also been surveyed. The research issues remain wide open for future investigation, and find the best technique is range free distributed positioning scheme because its provide the large scale range and range free technique at present time .

REFERENCES

[1]. Ian F. Akyildiz , Dario Pompili, TommasoMelodia, "Underwater acoustic sensor networks: research challenges", Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA.

[2]. Weichao Wang, Jiejun Kong, "Visualisation of wormholes in underwater sensor networks: a distributed approach", Int. J. Security and Networks, Vol. 3, No. 1, 2008.

[4]. "Securing Underwater Wireless Communication Networks", Electrical and Electronics Engg. Seminar Report 2013.

[5]. Ashvini P. and Sivasankaran V., "Securing Underwater Wireless Communication Networks-Literature Review", ARPN Journal of Engineering and Applied Sciences .©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.

[6]. Suraj S. Kasture, Nikhil Gudpelliwar, "Securing Underwater Wireless Communication Networks-Literature Review", Ashvini P. and Sivasankaran V. Department of Electronics and Communication System, Arunai College of Engineering, Thiruvannamalai, India.

[7]. Guangjie Han,1,2Jinfang Jiang,1,2 Lei Shu,3 Yongjun Xu,4 and Feng Wang5Sensors (Basel). 2012; 12(2): 2026–2061. Published online 2012 Feb 13. doi: 10.3390/s120202026.

[8]. Samedha S. Naik1, Manisha J. Nene2, "REALIZATION OF 3D UNDERWATER WIRELESSSENSOR NETWORKS AND INFLUENCE OF OCEANPARAMETERS ON NODE LOCATION ESTIMATION", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012