Fuzzy Based Malicious Detection Approach For Underwater Ad-Hoc Wireless Network (UANET)

Ekta Deshmukh Bisen[1], Neeta Nathani[2], Dhananjay Bisen[3]

[1] PG Scholar, Deptt. of ECE, GGCT Jabalpur, M.P, India, ekta.deshmukh2105@gmail.com
[2]Assistant Professor, Deptt. of ECE, GGCT Jabalpur, M.P, India, neetanathani@ggct.co.in
[3]Assistant Professor, Deptt. of IT, UIT-RGPV Bhopal, M.P, India, bisen.it2007@gmail.com

Abstract: Fuzzy logic based efficient malicious detection approach (FL-EMDA) has introduced for underwater ad-hoc wireless network (UANET) in which ad-hoc network scenarios create within underwater situation and use AODV routing protocol. This is done through design of fuzzy inference system (FIS) for identifying malicious behavior of node. FIS uses three input parameter packet delivery ratio, packet forward and residual energy of node. FIS classifies the network nodes weather it is malicious or not with the help of these inputs. The proposed algorithm will identify the above discussed activities and it will also discover a trusted path for secure data transmission. After detection of malicious nodes using FIS, simulation results are performed by parameters such as packet delivery ratio, average throughput and total packet forwarding with variation of malicious nodes. Comparative analysis proves that the proposed system is well suited for classification of mobile nodes and detection of malicious nodes within UANET.

Keywords: UANET, FIS, Malicious node, Fuzzy logic, MANET.

1. INTRODUCTION

Wireless technology is one of the most popular requirements of today's world. In wired network transformation of data achieved by physical transmission wires or links but in wireless network data transformation done via radio channels. All nodes shares same radio channel and exchange data with other nodes. In recent years the use of Ad-Hoc Network rises tremendously. Ad-hoc network is an infrastructure less self configured network in which mobile devices connected with the help of wireless medium without the need of internet connection between them [1]. Large-scale Underwater Ad-hoc Networks (UANET) and Underwater Sensor Networks (UWSN) are narrative networking paradigms to explore the uninhabited oceans shown in Figure-1. However, the characteristics of these new networks, such as huge propagation delay, floating node mobility, and limited acoustic link capacity, are significantly different from ground-based mobile ad-hoc networks (MANET) and wireless sensor networks (WSN). Over the past few years, there has been a quickly rising research topic on underwater adhoc network due to its broad applications within many scenarios, like gathering or compilation of data for oceanographic analysis, assisted navigation, predication of data for navigation and disaster prevention etc. In this work, mobile ad-hoc network creates underwater conditions within wireless enabled submarines and more than one submarine can communications with each other without any central authority [2] [3].

A fuzzy inference system is fuzzy logic rule based model which is used for classification of mobile nodes of UANET in proposed work. FIS takes decision and generate output in the same manner as human mind does. In FIS scalar values of input parameters first of all converted in fuzzified values. After that numerical manipulation with different linguistic fuzzified values using membership function and fuzzy rules performed. The decision making system generates suitable decision on the basis of these rules. After that fuzzified output converted back into scalar values. FIS has been taken up to make control decision to improve the performance or to improve the problem that conventional theory failed to attain success. In a network uncertainty due to mobility, unstable links, limited resources, energy constraint and node security are the most popular issues of ad-hoc network.

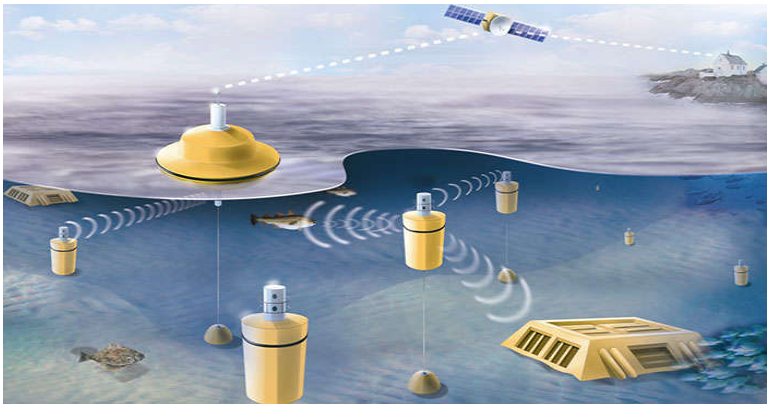

Figure 1: Underwater communications between submarines

2. RELATED WORK

UANET use routing protocol for communication like MANET. There are mainly available in three form, which are proactive routing protocol (table driven), reactive routing protocol (on demand) and hybrid routing protocol. Selection of routing protocol is most important fundamental issue of MANET. They should have the capability to fulfill requirements such as high power consumption, low bandwidth utilization, high error rate and unpredictable movements of node. AODV routing protocol is a reactive routing protocol that generates route identification process only when needed which reduces the workload of the network. AODV router receives a request message after that it cross checks its routing table and identify the availability of desired route [2]. If route is found then AODV forwards the message to next node otherwise it saves message and begin a route request procedure to find route to update own routing table for future use. AODV routing protocol search for shortest optimal path to exchange data between source and destination node but attacker nodes try to confuse source node to collect original data to destroy the linearity of the network. Whole networking function of UANET such as routing, packet forwarding and receiving all operations are performed by nodes in self organizing manner that's why security of mobile Ad-Hoc network is very challenging issue [4].

Dini G. and Duca A. L. [4] in 2012 proposed the underwater secure communication suite for UASNs. This was designed and experimented within the European project called "Underwater Acoustic Network" (UAN). Kong Jiejun et al. [5] proposed the Large-scale Underwater Ad-hoc Networks (UANET) and Underwater Sensor Networks (UWSN) are novel networking paradigms to explore the uninhabited oceans. In this paper adopt a top-down approach to explore the new research subject. In this paper the attention to build large-scale UANET and UWSN for real-time aquatic applications. Domingo M. C., Barcelona Tech University [6] in 2011 proposed 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 and the differences between underwater sensor networks and their ground-based counterparts require the development of efficient and reliable security mechanisms.

Das A. P. and Thampi S. M. [7] in 2015 proposed various Denial of Service attacks in mobile UWSNs. That simulated a flooding attack and an out-of-coverage problem caused by mobility by using Aqua-Sim, and analyzed their impact on UWSN performance. Han Guangjie et al. [8] in 2015 proposed a somewhat comprehensive survey of the emerging topics arising from secure communications in UASNs, which naturally lead to a great number of open research issues outlined afterward, and focused on the unique characteristics of the acoustic communication channel, and studied possible attacks and countermeasures of communication protocols in UASNs. Lal C. et al. [3] IEEE in 2017 proposed the wireless nature of the acoustic medium makes UANs vulnerable to various malicious attacks yet limited consideration has been given to security challenges. In this paper, outline of a hybrid architecture represented that incorporates aspects of physical layer security, software defined networking, node cooperation, cross-layering, context-awareness and cognitions.

M. R. Ahmed [9] in 2015 also proposed support vector machine to identify malicious attack in UWSN. Future work is addressing these issues to move toward the implementation and validation of the proposed solutions through computer simulations.

Ateniese G. et al. [10] in 2015 proposed and introduce Sec FUN, a security framework for underwater acoustic sensor networks (UASNs). Despite the increasing interest on UASNs, solutions to secure protocols from the network layer up to the application layer are still overlooked. Harris A. F. and Zorzi M. [11] proposed the underwater environment differs from the terrestrial radio environment both in terms of its modem energy costs, and in terms of the channel propagation phenomena. Xiang-ping G., Yana Y., Rong-lin H. [12] proposed in 2011 Underwater wireless sensor networks is composed of a variable number of sensor networks that communicated with each other using acoustic signal and the sensor nodes are deployed in some special underwater environment for monitoring tasks. Recently fuzzy based systems also gained attention in realizing different goals on this domain [13] [14] [15]. In this paper FIS is adopted to solve node security issue of ad-hoc network by classifying mobile nodes.

3. Proposed work of FL-EMDA

This section describes the working of the proposed FL-EMDA with algorithms employed at different modules. There are two basic modules in proposed approach:

1. Analyzing module
2. Malicious identification module

3.1 Module 1: Analyzing Module

In the Analyzing Module creates and analyze the adhoc network within underwater condition. Detailed procedure is given in algorithm-1 given below:

Algorithm-1

Step 1: Create Underwater Ad-hoc Network that uses following configurations:

a. Underwater channel model (Acoustic Channel) "Channel/UnderwaterChannel" in the TCL script. This employ default average salinity value 35 parts-per-million. The frequencies associated with underwater acoustics are between 10HZ and 1MHZ. The sound speed is 1500m/s this is lower than radio and optical propagation.
b. Underwater propagation model "Propagation/UnderwaterPropagation" included in TCL.
c. Underwater physical model "Phy/UnderwaterPhy" in the TCL script. By default set the maximum transmit power and the receive threshold.
d. Initially, nodes are configured with random assignment of mobility and create connections between source to destination nodes with random energy.

Step 2: Multiple sender (SN) and destination nodes (DN) define in network and AODV routing protocol configures to create route between them.

Step 3: In AODV routing, when sender node wants to communicate with the destination node then

- If destination node comes under the transmission range of source node then SN direct communicates with DN.
- Otherwise source node uses intermediate (peer) nodes (IN) for packet forwarding to DN.

Step 4: To create effective routing for packet transmission, source node initially broadcasts Route request packet (RREQ) to its intermediate nodes.

(a) If (Node = = IN && Packet = = RREQ)
Send Acknowledgment to SN
(b) If (IN = = valid node)
Use in routing process and SN can transmit data
Otherwise
IN may be malicious node and go to step 11 (Module II)

Step 5: Each intermediate node check following condition:

If (Neighbor of IN = = DN)
IN won't transmits RREQ again
Only data packet can be forwarded to DN and go to step 7
Otherwise
IN again broadcasts the RREQ control packet to their neighbor and increase hop count
And step 6 is repeated

Step 6: Finally destination node (DN) sends route reply packet (RREP) through IN to SN and connection is established.

If (DN = = True)
Reply RREP (unicasting) to SN
SN can send data packets
Otherwise
Repeat step 5

Step 7: Intermediate nodes are configured with random mobility therefore sometime communication link between source and destination can be changed.

If (any IN moves from routing path or dead due to less energy)
Previous node broadcast Route Error packet to SN
Otherwise
Continue packet transmission (Repeat step 5)

Step 8: Initially using previous steps simulation of UANET is done in analyzing module and analyzes performance of each node in the form of trace record.

Step 9: After analysis of trace record, performance of UANET is calculated in following terms:

a. Packet delivery Ratio in variation of number of malicious nodes
b. Throughput in variation of number of malicious nodes
c. Packet loss Rate in variation of number of malicious nodes

3.2 Module II: Malicious identification Module

In this module, fuzzy inference system (FIS) is defined for identifying malicious behavior of node. It includes three performance parameter of each node as an input like packet delivery ratio (PDR_N), packet forwarding ratio (PFR_N) and residual energy (RE_N) of node. These inputs are mapped in single output weather it is malicious node or normal node. In this work, FIS is working like classifier that classifies the network nodes with the help of these inputs. Fuzzy inference system is consisted of some basic steps such as input variables, fuzzification process using membership function, define knowledge base or rule base for mapping input into output and defuzzification process.

After defuzzification, final values are converted into crisp values corresponding to each node. When that calculated value of node come under the threshold value then that node consider as malicious node from table 1.

If (node_value <= 0 && node_value <= 0.4)

Node will consider "Malicious node" that can eliminate from the network

Otherwise

Node can be good and it can use for routing process

After elimination of malicious node, again simulation is performed with same configurations and parameters and results compare with previous results and for this process repeat steps 8 and 9 of Algorithm-I.

Table 1: Rule Base

PDF / PFR	Residual Energy (RE)		
	Low	**Good**	**Best**
Low	Low	Good	Good
Good	Best	Best	Best
Best	Best	Best	Best

4. SIMULATION RESULTS AND ANALYSIS

Simulation is a fundamental tool which is used for the development of the Ad-hoc network. The simulation provides freedom from difficulty of analyzing and verification of protocol for large scale systems. It provides flexible opportunity to test system with different topologies, mobility patterns along with several physical and network layer protocols. In Ad-Hoc network routing protocol adapted according to requirement of the network and experience high variability in performance under certain conditions. Simulation provides opportunity to understand that how the changes impact the performance result of the network. There are well known simulators used for the simulation of UANET which are QualNet, NS-2, GloMoSim and OPNET, DIANEmu, GTNets, J-Sim, Jane, NAB, OMNet++ and SWANS. NS-2 simulator adopted for simulation in this dissertation. After analyzing network by NS-2 a trace file generated [16]. Three parameters such as packet delivery ratio, packet forwarding and residual energy are considered as an input for FIS. Fuzzy logic toolbox provides MATLAB functions [17], graphical tools and simulation link blocks for analyzing, designing and simulating system based on fuzzy logic. In this work all the simulation work is performed in NS-2 wireless network simulator version 2.35.

4.1 Network Configuration

- Channel Type: Channel/Underwater Channel
- Radio-propagation model: Propagation/ Underwater Propagation
- Network interface type: Phy/WirelessPhy
- MAC type: Mac/802_11
- Interface queue type: Queue/DropTail/PriQueue
- Antenna model: Antenna/OmniAntenna
- Max packet in Queue: 50
- Total Number of Mobile Nodes: 50
- Routing protocol: AODV
- Topography Dimensions: 1000X1000
- End Time of Simulation: 100 sec
- Initial Node Energy: 300 joules
- Traffic flow between nodes: UDP/CBR
- Packet Size: 512 kb

- Data Rate: 8 kbps
- Node Speed: 5m/s, 10m/s, 15 m/s, 20m/s, 25 m/s

4.2 Dynamic Connection Patterns

"/home/neeti/ns-allinone-2.35/ns-2.35/indep-utils/cmu-scen-gen/setdest/scen-5-10-test"

To create Dynamic connection pattern use following commands

./setdest -Version –Number of Node –Speed Type-Min Speed- Max Speed- Simulation Time- Pause Type- Pause Time- X dimension –Y dimension

Example: ./setdest -v 2 -n 50 -s 1 -m 5 -M 20 -t 100 -p 1 -P 10 -X 1000 –Y 1000

Effect of Malicious Node:

Calculation of packet delivery ratio and average throughput for normal case with presence of malicious node and without malicious node

The following percentage of malicious nodes is presented in network.

1. If 2% nodes work like malicious.
2. If 4% nodes work like malicious.
3. If 6% nodes work like malicious.
4. If 8% nodes work like malicious.
5. If 10% nodes work like malicious.

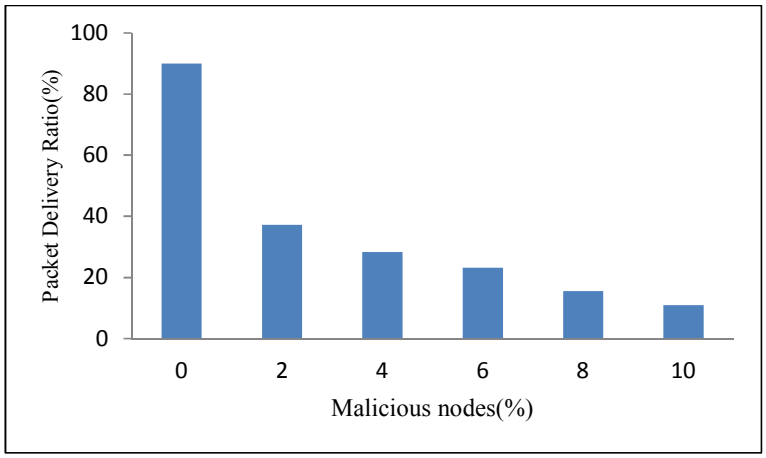

Figure 2 Packet Delivery Ratio Vs Malicious Node

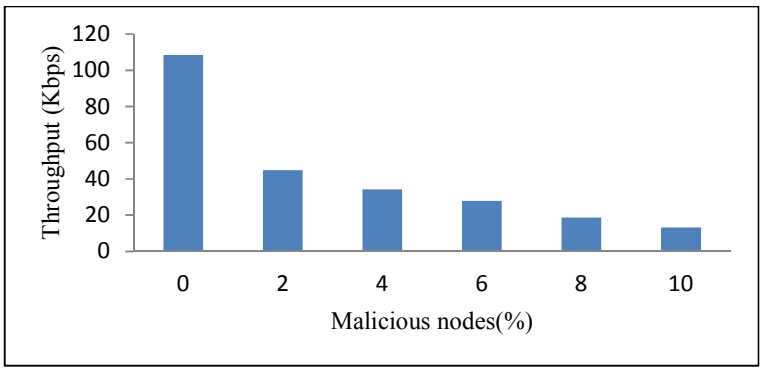

Figure 3: Average Throughput Vs Malicious Node

Packet delivery ratio is calculated by ratio of received packet and sending packets. The above figure 2 represents effect of packet delivery ratio with the present of malicious nodes. As we have seen that when number of malicious nodes increasing in the network then packet delivery ratio is reducing. It means number of drop packets is increases due to malicious node. In this scenario malicious node receives the packet but they do not forward packets to other nodes and they are dropping all the received packets. It also affects the average throughput of network shown in figure 2. It is calculated by total bit transmission per second. In this scenario all the values are calculated in kbps and when malicious nodes increasing then transmission rate in bits per second is also reducing.

Effect of malicious node on Packet loss Rate in presence of 100 nodes

In Figure 4, it can be observed that when percentage of malicious nodes increases, proposed approach gives higher PDR compared to other. This is defined to fact that AODV has no defensive mechanism for identifying malicious nodes. In fact, the packet dropped rate analyzed by previous methods within different condition is higher as compare to proposed FL-EMDA.

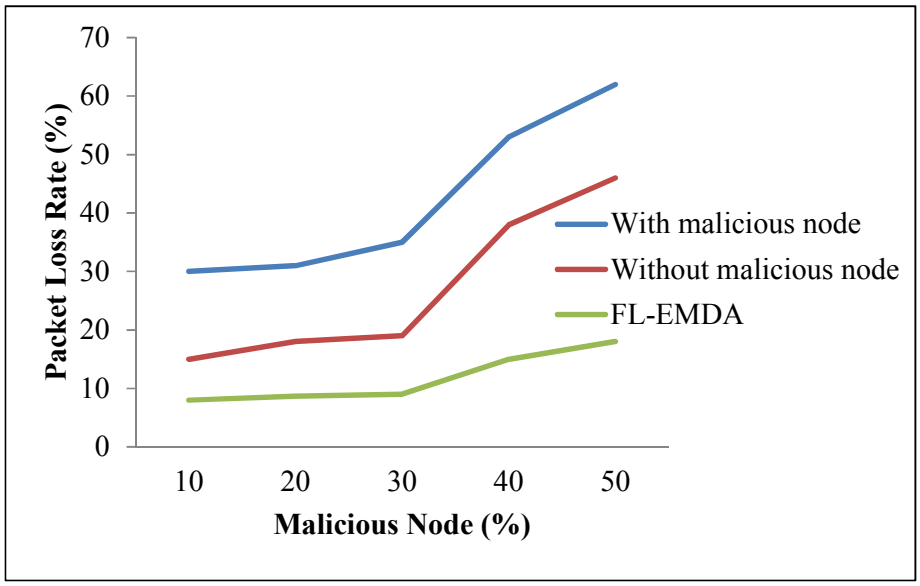

Figure 4: Packet Loss Rate (%) Vs Malicious node (%)

5. CONCLUSION AND FUTURE DIRECTIONS

Mobile Ad-Hoc Networks has the capability to organize a network where a conventional network base environment cannot probably be deployed. Security of UANET is most significant feature for its operation. In this thesis work fuzzy logic based approach named fuzzy inference system has been deployed for UANET. To increase the performance of the network fuzzy inference system adopted to identify malicious nodes in the network. In this proposed system, fuzzy logic based efficient malicious detection approach (FL-EMDA) has introduced for underwater ad-hoc wireless network (UANET) in which adhoc network scenarios create within underwater situation using AODV routing protocol. The simulation results are evaluated by varying node speed and by varying packet interval in presence, absence of malicious nodes and after detection of these nodes using FIS. The proposed method is compared with conventional method and better results are analyzed. It can be concluded that fuzzy inference system has intense capability to develop highly efficient network environment. In future, this proposed fuzzy inference system could be analyzed on the basis of other parameters to detect other kind of malicious activities.

REFERENCES

1. C. S. R. Murthy, B. S. Manoj, "Ad-Hoc Wireless Networks: Architecture and Protocols", Pearson Ltd, 2004.
2. I Chlamtac, M Contj, and J Liu, "Mobile ad hoc networking: imperatives and challenges," Ad-hoc Networks, vol. 1, no. 1, pp. 13-64, 2003.
3. C. Lal, R. Petroccia, K. Pelekanakis, M. Conti and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," in IEEE Journal of Oceanic Engineering, vol. 42, no. 4, pp. 1075-1087, Oct. 2017.
4. G. Dini and A. Lo Duca,, "A Secure Communication Suite for Underwater Acoustic Sensor Networks." Sensors vol. 12, no. 11, 15133-15158, 2012.
5. J. Kong, J.-hong Cui, D. Wu and M. Gerla, "Building underwater ad-hoc networks and sensor networks for large scale real-time aquatic applications," MILCOM 2005 - 2005 IEEE Military Communications Conference, Atlantic City, NJ, Vol. 3, pp. 1535-1541, 2005.
6. M. C. Domingo, "Securing underwater wireless communication networks," in IEEE Wireless Communications, vol. 18, no. 1, pp. 22-28, February 2011.
7. A. P. Das and S. M. Thampi, "Secure communication in mobile underwater wireless sensor networks," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, pp. 2164-2173, 2015.
8. G. Han, J. Jiang, N. Sun and L. Shu, "Secure communication for underwater acoustic sensor networks," in IEEE Communications Magazine, vol. 53, no. 8, pp. 54-60, August 2015.
9. M. R. Ahmed, S. M. Tahsien, M. Aseeri and M. S. Kaiser, "Malicious attack detection in underwater wireless sensor network," 2015 IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, pp. 1-5, 2015.
10. G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli and D. Spaccini, "SecFUN: Security framework for underwater acoustic sensor networks," OCEANS 2015 - Genova, Genoa, pp. 1-9, 2015.
11. A. F. Harris, M. Zorzi Poster Abstract: Modeling the Underwater Acoustic Channel in ns2, Presented as a poster in WUWNet '07, 2007.
12. G. Xiang-ping, Y. yana, Hu Rong-lina, "Analyzing the Performance of Channel in Underwater, Wireless Sensor Networks (UWSN)", Procedia Engineering, vol. 15, 95-99, 2011.
13. D. Bisen and S. Sharma, "Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET" Natl. Acad. Sci. Lett., 2017, https://doi.org/10.1007/s40009-017-0602-1.
14. D. Bisen, S. Sharma, "An enhanced performance through agent-based secure approach for mobile ad hoc networks", International Journal of Electronics, Vol. 105, Issue 1, 2018.
15. N. Thakur, D. Bisen, & N. Gupta, "Proposed agent based black hole node detection algorithm for ad-hoc wireless network", International Journal on Computational Science & Applications, Vol. 5, Issue 2, pp. 69–85, 2015. doi:10.5121/ijcsa.2015.5207
16. The Network Simulator ns-2. (2017). Information Sciences Institute, USA. Viterbi School of Engineering, September. Retrieved from http://www.isi.eu/nsnam/ns/
17. Matlab (2017):http://in.mathworks.com/products/fuzzy-logic/.