SECURITY CONSIDERATIONS IN A MARINE COMMUNICATION NETWORK FOR FISHERMEN

Dhaneesh B Nair[1], Dhanesh Raj[2], Sethuraman Rao[3]

Amrita Center for Wireless Networks and Applications, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Kollam, Kerala, India.

ABSTRACT

With the recent advancements in and popularity of wireless networks, the security based issues are also increasing considerably. In this paper, we look at the data security and situational security vulnerabilities in the communication network for fishermen at sea being developed by our research center. We are proposing certain solutions and algorithms for avoiding some of the situations. They are Adaptive Context-aware Transmission Power Control (ACTPC) as a proposed solution for preventing unauthorized users at the maritime border, along with border alert and distress alert. The algorithms are implemented using a network of MICAz motes.

KEYWORDS

MANET, ACTPC, CPE, AP, NOC

1. INTRODUCTION

Currently, Indian fishermen need to use either handheld wireless radio or satellite phones for communication. Neither of these options are cost-effective. In addition, handheld radios are broadcast based and their range is also restricted to LoS. Hence, no viable means of communication exist for the majority of Indian fishermen when they spend several days together at sea. For this reason, a project is underway at our research center to develop a communication network to serve their needs. The project is titled Mobile Infrastructure for Coastal Region Offshore Communications & Networks (MICRONet). The network will consist of clusters of boats forming a wireless mesh network amongst them. These clusters will be connected to the base station on the shore using hierarchical point to multi-point backhaul links based on Long-Range (LR) Wi-Fi technology [2] [4]. Note that LR Wi-Fi uses TDMA MAC [3] [5]. The base stations on the shore will be connected to the internet thereby providing internet connectivity to the whole network. Each boat will have an Access Point (AP) to which the users in the boat will connect their devices such as smart phones, laptops, etc., wirelessly. Some boats will have a CPE (Customer Premises Equipment), which will provide the LR Wi-Fi backhaul link to the base station on the shore. A Network Operations Center (NOC), used for proper authorization, tracking and other network management services, will also be located on the shore. A boat may also act as a base station and provide a P2MP link in order to extend the coverage of the backhaul network. This is how hierarchical P2MP backhaul is achieved. A brief overview of the basic architecture is shown in Figure 1.

Thus, whenever any user in a boat needs to communicate with the land base station, the data will pass through the AP and one or more CPEs located on separate boats before it reaches the base station on the shore. The boats are mobile at a speed of 8-15 kmph. This will result in boats

DOI: 10.5121/ijci.2015.4202

frequently joining and leaving the clusters which form the wireless mesh networks. This will also mean CPEs associating and disassociating with the base stations frequently. Even though there are several infrastructure nodes in this network such as APs and base stations, the dynamic nature of both the access and the backhaul layers of the network make it susceptible to some of the security issues prevalent in a MANET [6]. In addition, there are certain security considerations that are specific to this application scenario. These pertain to both data security and situational security. This paper describes all these issues in detail and also proposes solutions to some situational security issues.

In our proposed communication network for fishermen at sea, an attacker boat can access or change the wirelessly transmitted data, malicious nodes in the network can damage the network topology and can destroy the communication, any attacker boat can route the transmitted data to different destinations, etc. So, a proper security system is required for the proposed network. We need to address the potential security vulnerabilities in the proposed network and provide effective solutions for security drawbacks in different layers of protocol stack. In addition we need to address situational security issues such as preventing unauthorized users at the maritime border, border alert, distress alert, etc.

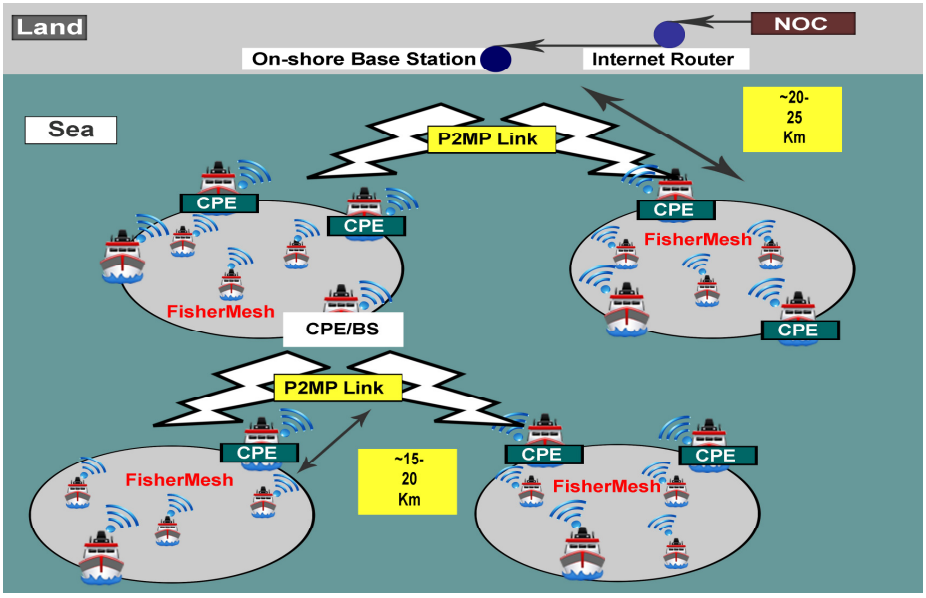

Figure 1. MICRONet Architecture

2. RELATED WORK

Since MANET suffers from lack of infrastructure, there are many security vulnerabilities in MANET. These have been studied thoroughly over the years. In the case of MANET, there will be different types of attacks [8] happening from Physical layer to Application layer.

Jiwen CAI [1] proposed an efficient algorithm for detecting black hole and gray hole attacks in ad-hoc networks, which is tested using DSR protocol in ns-2 simulator. Here, they proposed a path based method to overhear the next hop's action and false positive rate is reduced by establishing a collision rate reporting system. The paper presents an innovative approach for detecting black hole and gray hole attacks by modifying the detecting threshold according to the network overload and using cross layer design to improve the performance. They compared their

method to other strategies, and confirmed that their proposal provided better detection. We can use a similar approach in this project to detect network layer attacks.

Mohammad Wazid [19] surveyed attacks at different layers and some of the available detection techniques such as intrusion detection technique, Cluster based intrusion detection technique and misbehavior detection through cross layer analysis. In the intrusion detection technique, every node participates in the detection process. It has four functional modules such as Local data collection module, Local detection engine, Cooperative detection engine and Intrusion response module. In order to avoid the participation of every node, Cluster based intrusion detection technique is established and to detect the cross layer attacks, cross layer mechanism is established in misbehavior detection through cross layer analysis method. Some of the attacks analyzed in this survey are applicable to our scenario.

Amol A. Bhosle [20] proposed a method for detecting black hole and wormhole attacks in routing protocol AODV in MANET. In this, he has proposed a watchdog mechanism and a time of flight technique for avoiding black hole attack and wormhole attack. The paper presents a good routing algorithm for improving the data security. In modified AODV, each node needs to have more memory and if transmission failure occurs in a node due to any reason, there is a chance for other nodes to treat it like a misbehaved node.

J. Godwin Ponsaml [21] surveys the overall security challenges or issues and their solutions in every layer in a communication path starting from physical layer to application layer in MANET communication. In the physical layer, spread spectrum technologies such as FHSS or DHSS can be used to prevent eavesdropping attacks. Traffic analysis is prevented by encryption at Data link layer. LLSP is used to provide security at Link layer. SLSP is used to prevent DOS attack and man in the middle attack. In network layer, ARAN is used to defend impersonation and repudiation attacks. Security protocol SEAD is used against modification attacks. In Transport layer, SSL protocol implements end to end security for a session. In the application layer, firewalls can prevent many attacks. Also an IDS system can be used as a second line of defense. From this survey, many security challenges and solutions pertinent to our scenario can be identified.

Dr. M.S. Aswal [22] wrote a review paper discussing the challenges in Wireless Mesh Networks and recommended some of the possible counter measures such as cryptography, pair-wise key sharing and secure routing. Hariom Soni [11] surveys different routing protocols in MANET, Mike Burmester [16] details about the route discovery security in MANET and talks about the route discovery algorithm endairA. Satria Mandala [12] does a survey of the intrusion detection algorithms in MANET. Sarvesh Tanwar [18] surveys various problems and security issues in ad-hoc networks.

P. Visalakshi [17] discusses about the various security issues in MANETs and some of its countermeasures. The paper describes about the behavior of malicious nodes. Then various vulnerabilities in MANET like unsecured boundaries, compromised nodal threat, non-availability of centralized management facility, limited power supply and scalability are discussed. Existing security solutions such as traffic flow monitoring, trust, cluster based IDS and cross layer detection mechanisms are evaluated. The paper describes some of the attacks and their solutions and the authors are generalizing the MANET attacks.

U. Sharmila Begam [15] talks about secure intrusion detection systems in MANET and describes a new intrusion detection technique, EAACK. B.Praveen Kumar [13] presented a survey on different MANET security problems and different MANET routing protocols. Manjeet Singh [14] surveys different types of attacks that are possible in MANET irrespective of different layers. K.

Muthukumaran [9] evaluates different issues and security vulnerabilities in different layers of MANET. Alex Hinds [10] reviews different routing protocols for MANET.

Saloni Sharma [7] does an all round evaluation of different security issues and different routing protocols and issues in MANET.

Based on these papers, we are analyzing various potential threats that can happen in the network being formed at sea and also proposing solutions for certain situational security issues in the communication network.

3. ISSUES IN THE COMMUNICATION ENVIRONMENT

3.1 Generic Attacks at Various Layers of MICRONet Architecture

3.1.1 Physical layer attacks

3.1.1.1 Jamming attack

The messages sent to the Access node or CPE can be lost or corrupted by jamming attack. The attack is done by sending powerful radio signals to the Access node or CPE so as to block any signals coming towards it.

3.1.1.2 Eavesdropping attack

From Smart phone to Access node or from CPE to CPE, any intruders can tune to the same frequency and listen to the transmitted signals during message transfer.

3.1.1.3 Malicious message injecting

In this attack, attackers inject fake messages along with the actual message during the transmission of the signals. Thus the functionality of the network will get interrupted by the intruders.

3.1.2 Data link layer attacks

3.1.2.1 MAC Denial of Service attacks

Any attacking boat or node can continuously keeps the channel busy or the intruder can continuously send unnecessary packets to any particular access node or CPE so as to drain its battery.

3.1.2.2 Bandwidth Stealth

Congestion will happen in the network when an attacker steals a large fraction of the bandwidth.

3.1.2.3 Resource exhaustion

Intruder nodes make continuous repeated collision to drain the battery power.

3.1.2.4 WPA2 targeted attack

WPA2 is the strongest security protocol available for the wireless network. Still there are some loopholes such as Hole196 to breach the security provided by the protocol.

3.1.2.5 Traffic monitoring

By monitoring the traffic flow, an intruder can perform analysis of the type of communication happening in the network.

3.1.3 Network layer attacks

3.1.3.1 Flooding attack

Network performance degradation is done by continuously sending RREQ messages to any particular node in a short duration of time by any attacker element or continuously engaging the access node or CPE to work without an interval so as to exhaust the network resources and bandwidth.

3.1.3.2 Routing table poisoning attack

Routing tables can be modified by any intruder so as to have improper routing and routing towards any particular destination.

3.1.3.3 Sleep deprivation attack

By asking for non-existing node destinations, any attacker node can waste the resources like bandwidth and battery power of any particular node.

3.1.3.4 Impersonation attack

Any attacker boat can impersonate as a registered boat and can cause attacks.

3.1.3.5 Node Isolation attacks

In this attack, isolation of the registered boats is done to prevent communication between boats.

3.1.3.6 Message modification

Modification of the transmitted message can be done by adding false stream of messages as pulses along with the actual information.

3.1.3.7 Black hole attack

Any intermediate attacker node can act as an element in the routing path and can drop all the packets passing through it.

3.1.3.8 Wormhole attack

In this type of dangerous attack, attacker node establishes a virtual high speed route to the destination so that the attacker can take away and modify the data from the route without any knowledge of the actual nodes.

3.1.3.9 Link Spoofing attack

The malicious nodes advertise fake route links to other nodes in order to disrupt routing operations.

3.1.3.10 Byzantine attacks

In this attack, one or several malicious nodes form a group and produce combined attacks.

3.1.4 Transport layer attacks

3.1.4.1 TCP session hijacking

The malicious node takes the characteristics of the victim node by spoofing its IP address and steals the information communicated with the victim node.

3.1.4.2 Jelly Fish attack

This attacker gets into the routing path and drops or delays the packets passing through it. Thus it causes packet drops, delay or jitter at the receiver.

3.1.5 Application layer attacks

3.1.5.1 Repudiation attack

Due to this attack, whole communication is affected from denial of participation.

3.1.5.2 Attack by virus and worms

Operating system installed in CPE and access node can be affected by virus and worms.

3.2 Issues Specific to MICRONet Marine Communication Environment

3.2.1 Signal crossing the maritime border

In the case of boats close to the maritime border, signals going from the boat can go beyond the maritime border, since the transmission range of each antenna will be very high due to the usage of Long range Wi-Fi technology. Thus, the signals going out of the border can be accessed by malicious people from any neighbouring country. Also, boats from neighboring country will be able to access the internet connection provided from the shore assuming they could somehow authenticate themselves. Thereby, neighboring country boats will be able to access certain sites that should be accessible only within the country.

3.2.2 Boats crossing the maritime border

Fishing boats will be moving deep into the sea so that if the boats don't get any maritime border information, there is a high chance for the boats to cross the maritime border.

3.2.3 On-boat AP attacks

3.2.3.1 Local Wi-Fi security attacks

Communication between smart phone and access node takes place by short range Wi-Fi technology with WPA2 as the security protocol and will be facing the common security issues.

3.2.3.2 AP Spoofing

Attacks like Hole 196 can happen in the network which is due to spoofing of AP by any of the users in the boat or by any malicious node nearby.

3.2.4 Off-boat AP attacks

3.2.4.1 AP Spoofing

3.2.4.2 Delaying of packets

Packets from other boats can be delayed by the boats in the routing path while having on-boat AP to off-boat AP connection.

3.2.4.3 Attacks like Black hole and Wormhole attacks

While routing packets from any source boat to destination server, the nodes like boat APs or CPEs can drop, modify or mislead the packets.

3.2.5 Cluster forming by malicious boats

Attackers can form a boat cluster as in the MICRONet architecture and can make other boats believe that it is a registered cluster and can produce attacks.

3.2.6 Physical distress

3.2.6.1 Attack by intruders in a registered boat

When some people with malicious intention get into a registered boat, they will be able to route their own packets through the access node of the boat. Also, they can capture packets passing through the router.

3.2.6.2 Natural issues happening to boats

Problems such as boat sinking, fire in the boat, etc can damage the boat and cause node failure.

3.2.7 CPE, Access node, Smartphone and Base station spoofing

Each of the nodes in the network such as CPE, Access node, Smartphone and base station can get spoofed by any malicious nodes.

3.2.8 Attacks in the AP to AP and AP to CPE transmission path

Any intruder nodes can produce attacks on the transmission path in the network.

3.2.9 Problem with the TDMA approach

Different CPEs contact the onshore base station using TDMA approach. In the centralized TDMA approach, one central coordinator node takes full responsibility for coordinating transmission in the whole network. So, by controlling the particular node, any malicious intruder can take control of the data flow of all other boats.

4. SOLUTIONS TO SOME SITUATIONAL SECURITY ISSUES

4.1 Adaptive Context-aware Transmission Power Control (ACTPC)

In order to prevent unauthorized access by intruders, as described in section 3.2.1, it is a good idea to ensure that the data traffic does not cross the maritime borders of the country. We do this by dynamically adjusting the transmission power level by sensing the location of the maritime

border and the locations of neighboring boats with respect to the maritime border. The algorithm used for this is Adaptive Context-aware Transmission Power Control (ACTPC).
There are two scenarios to consider. (i) When a boat acts as a base station to increase the range of the backhaul network. In this case, it is trying to serve boats that are in between itself and the maritime border. (ii) When a boat close to the maritime border is part of a wireless mesh network formed by a cluster of boats, i.e. access points. Scenario (i) is much more critical than scenario (ii). This is because while the backhaul link is expected to span 10-15 km, the wireless mesh network is expected to have a radius of 100-500 m. Refer Figure 1, Figure 2 and Figure 6.

Note that while the nodes in the backhaul network will have directional sector antennas, the nodes in the access network (wireless mesh network) will have Omni-directional antennas.
The proposed algorithm for scenario (i) works as follows:

a) All the boats being served by a base station (which could also be a boat) calculate their distance from the maritime border and send it to the base station at regular intervals (d(S_B)). For the sake of efficiency, they could piggy-back this information on some other control frame such as PS-Poll frame. The algorithm for calculating the distance from the maritime border is explained in section 4.1.1.
b) The base station boat calculates its distance from the maritime border (d(R_B)) using the distance calculation algorithm.
c) Then it calculates the difference value, d(S_R) of different boats and checks whether it is less than its distance from maritime border and calculates the maximum d(S_R) value, Max(d(S_R) such that it is less than its own distance from maritime border.
i.e., Difference, d(S_R) = Base station boat's distance from the border – CPE boat's distance from the border, as in Figure 2.
So, d(S_R) = d(R_B) – d(S_B)
d) Then the base station sets its transmission power level such that its range extends to Max(d(S_R)). An appropriate fade margin may be incorporated to account for the channel fade conditions.

The proposed algorithm for scenario (ii) is as follows:

a) The boats (access points) within a wireless mesh network exchange their distance from the maritime border at regular intervals preferably piggy-backing on a control message.
b) When a boat wants to send data back to the shore, it ensures that its nearest neighbor towards the shore is closer to it than its own distance from the maritime border and controls its transmission power level to reach its nearest neighbor towards the shore.
i.e., Difference, d(S_R) = Neighbor boat's distance from the border – Sender boat's distance from the border.
So, d(S_R) = d(R_B) – d(S_B)
S adjusts its transmission power level to cover Min(|d(S_R)|) provided.
Min(|d(S_R)|) < d(R_B) AND d(S_R)) > 0
c) If it does not find any neighbor within that range, it does not transmit any data. Instead, it generates an alarm to notify the boat to move further away from the maritime border towards the shore. This could be an audio or visual alarm or a combination of the two.

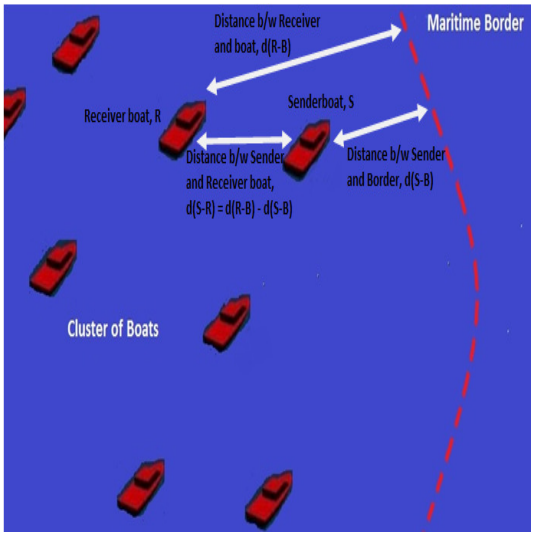

Figure 2. Cluster of boats near the Border

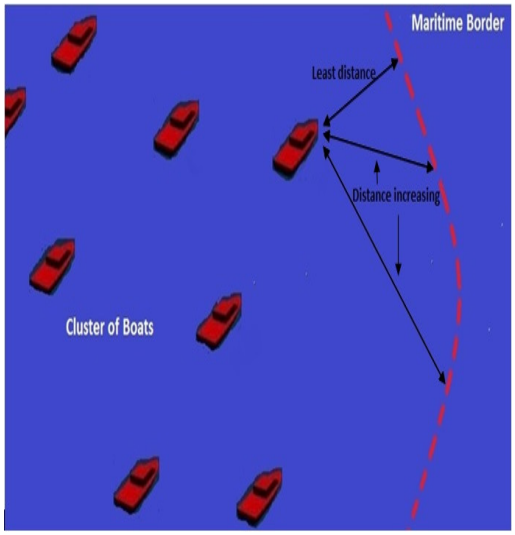

Figure 3. Variation of Border distance

4.1.1 Distance Calculation Algorithm

Every boat will be having on-boat GPS device for finding its location. So, using the GPS device, every boat will be getting its location co-ordinates (latitude and longitude co-ordinates). The maritime border for a country is always fixed and constant. Also, the border is not a straight line, which will be a well defined imaginary curve through the sea (Figure 3). When a CPE associates with a base station, it will get the maritime border segment corresponding to that region as an array of coordinates. Thus by knowing the maritime border co-ordinates and its current location co-ordinates, a boat will calculate its displacement from the maritime border by doing a binary search of the array of maritime border coordinates. The algorithm is described below:

a) Initially, choose the coordinates of the middle element of the array of border co-ordinates and calculate the distance from the co-ordinate to the boat.
b) Then, choose the immediate left and right co-ordinate points of the middle element and calculate the distance to those points.
c) If the distance of any one side is lesser, then continue with that half of the border.
d) Take the selected half as the whole border to be considered and perform steps (a) to (c) until the time you are left with an array size of 1 or 2 for the border.
e) If the array size is 1, calculate the distance of the boat from that point. If there are two points in the array, take the mean of the two distances.

4.2 Distress Alert

There can be different physical distress situations that can happen in a boat, as described in the previous section and the following procedure is used for broadcasting alert signals to all other boats and to the shore. Whenever any intruders get into the boat or any other distress situation arises, the fishermen can trigger an alarm by launching an app on their smart phone. This alarm message will be broadcast through the access node and CPE in the boat to every other registered boat at maximum power level. The alarm message will contain the type of alarm and the GPS coordinates of the boat under attack in addition to some other information. Thus, all other boats will learn about the attack on the particular boat and will relay the message to the appropriate security personnel through the base station. They will also stop routing their traffic through that boat by removing the particular boat's id from the forwarding tables. Refer Figure 4.

4.3 Border Alert

The distance from the maritime border will be periodically calculated using the distance calculation algorithm mentioned above and using that, whenever the distance from the border is less than a threshold value, say 100m, the boat will be alerted using an alarm in the boat as shown in Figure 5. This could be an audio or visual alarm or a combination of the two.

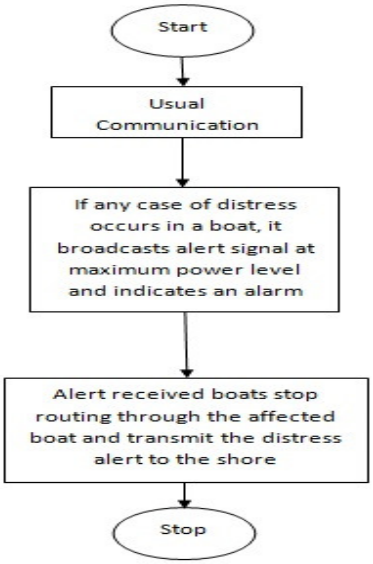

Figure 4. Distress alert flowchart

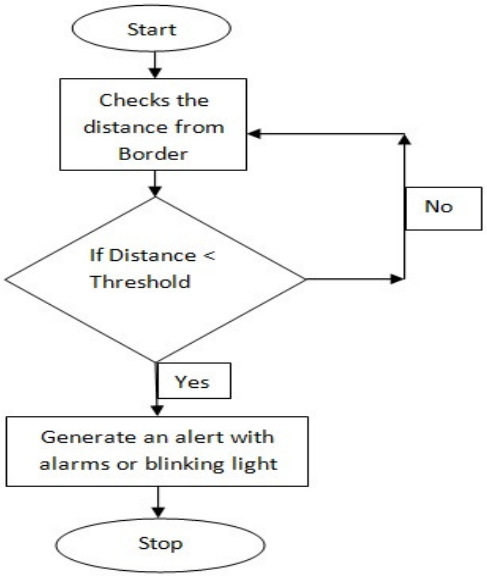

Figure 5. Border alert flowchart

4.4 Other common solutions

a) WPA2 security protocol is used for authentication and encryption, which will avoid node id spoofing attack, and other message decoding attacks.
b) Whenever an external unregistered boat is identified by a registered boat, it will send the information to NOC and all other boats.
c) Some of the physical layer attacks can be prevented by spread spectrum techniques.
d) Link layer attacks can be avoided by WPA2 encryption.
e) SAODV routing protocol can be used to prevent some of the network layer attacks.
f) In application layer, firewalls can effectively provide better security.

5. IMPLEMENTATION AND RESULTS

The algorithms for ACTPC, distress alert and border alert were implemented with the help of MICAz motes and MIB 520. We tested it with different number of nodes under various situations such as Sender boat having different distant neighbors, nodes facing distress condition, boat reaching nearer to the border and were able to successfully evaluate the scenario proposed. For the implementation, we have taken four different nodes, Sender node (node which needs to send the data), Receiver nodes (nodes which are in closest range to the Sender node), Receiver_0, Receiver_1, and Receiver_2 having node id's 1, 5, 2 and 4 and corresponding distance from the Maritime Border, 10, 5, 15 and 16. Each MICAz mote has its Power levels starting from 3 to 31 corresponding to the power levels -25 dBm to 0 dBm as shown in Table 1. The subset of implementation contains ACTPC algorithm procedures (Figure 6).

Every particular occurrence of the events will be shown by blinking appropriate LED. Initially, Sender node sends an 'init' message showing its request for establishing a route through any of the Received nodes. After getting the request, Receiver nodes acknowledge the signal received. The acknowledgement signals sent out by the Receiver nodes to Sender node will also be having their corresponding distance values from the maritime border.

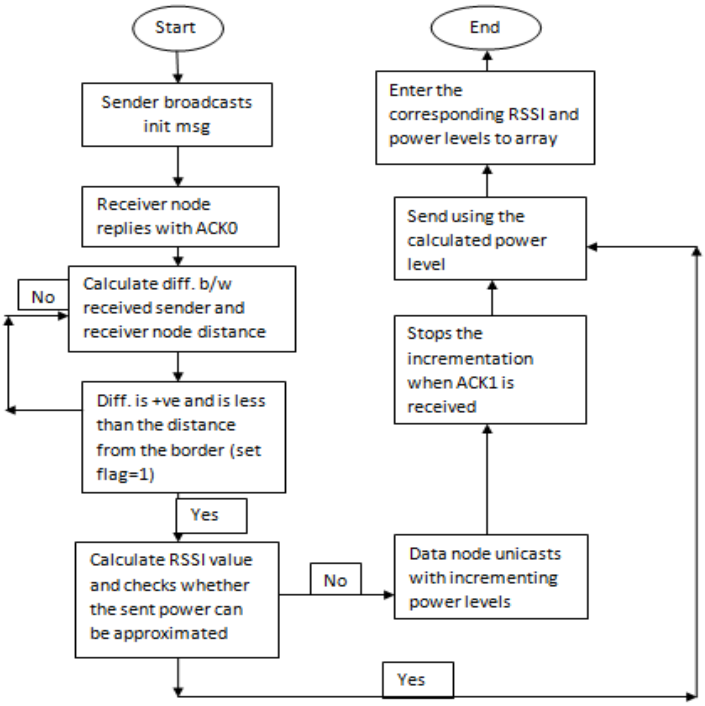

Figure 6. Main steps in ACTPC Algorithm

But the reply of Receiver node_0 will be received by Sender node initially since it is the nearest node. Then the Sender node takes the difference between Receiver node's distance and Sender node's distance and since it is negative (so, by sending data to the node will let the data to go towards the Border), the Sender node will not send the data to the Receiver node_0. Then, Sender node will get acknowledgment from Receiver node_1.

After calculating the difference, Sender node finds that it is between Sender node and shore. Then the Sender node will send its data from minimum to maximum power levels to the Receiver node_1 to arrive at the optimum power level. This value along with the corresponding distance of the neighbor is cached by the Sender for later use. The acknowledgment coming at a later time from the Receiver node_2 will be discarded as the Sender node already found the nearest node for sending its data. After reception, Receiver node_1 forwards the data to the Receiver node_2 for sending towards the shore. After 25 seconds of time, it is assumed that some distress event occurred in the Receiver node_1. So, it will broadcast the distress alert to all other nodes with maximum power and will stop further reception. After reception of the alert signal, all other nodes will forward the alert signal towards the shore. After analyzing occurrence of some distress event in the Receiver node_1, the Sender node will stop transmitting towards Receiver node_1 and starts forwarding data to the Receiver node_2.

Table 1. Discrete power levels of MICAz mote

MICAz Transmit Power level	Transmitted Power Level (dBm)
31	0
27	-1
23	-3
19	-5
15	-7
11	-10
7	-15
3	-25

Table 2. Actual output readings

RSSI (dBm)	MICAz Transmit Power Level
-79	3
-81	3
-82	3
-84	7
-87	7
-88	11
-89	11

Table 3. RSSI readings w.r.t actual power levels

RSSI (dBm)	Transmit Power Level (dBm)
-79	-25
-81	-25
-82	-25
-84	-15
-87	-15
-88	-10
-89	-10

After 30 seconds from the starting of communication, it is assumed that Receiver node_0 has reached towards the border. That is, the border distance from the Receiver node_0 will be less than 100m. The Received Signal Strength Indicator (RSSI) readings as seen by the Sender mote along with Transmit Power level to reach the particular Receiver mote will be calculated and sent through UART to Cutecom interface in TinyOS operating system. There is an inverse correlation between the distance of the neighbor and the RSSI of the received signal. Thus at the time of reception of any signal by the Sender node, by looking at the Cutecom display screen, we will be able to see the RSSI readings and its corresponding Transmit Power level readings. The output readings with respect to MICAz power level and RSSI (dBm) value are shown in Table 2. The readings and corresponding graph of RSSI and Transmit Power obtained after the experiment are shown in Table 3 and Figure 7 respectively. RSSI From the Transmit Power v/s RSSI graph, we can see that as the RSSI value decreases, the Transmit power increases.

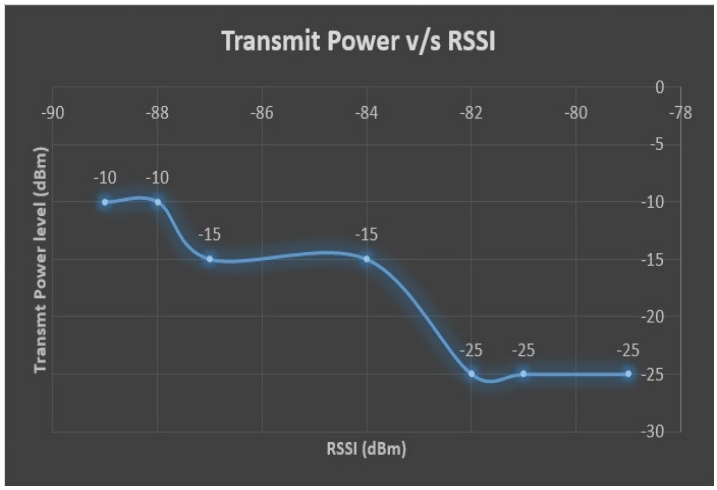

Figure 7. Transmit Power v/s RSSI graph

Thus, as shown by our implementation using MICAz motes, by using the Adaptive Context-aware Transmission Power Control algorithm, we can make the communication network of fishing boats more secure and robust against intrusions and other types of attacks.

6. CONCLUSION

Marine Communication Network for fishermen has many security issues and some of the major situational and data security issues and solutions were described. The proposed solutions for some situational security issues include Adaptive Context-aware Transmission Power Control (ACTPC) algorithm, distress alert and border alert mechanisms. ACTPC algorithm prevent boats from neighboring countries from accessing the internet service provided by this marine network. Border alert and distress alert mechanisms serve to improve the situational security of boats.

ACKNOWLEDGEMENT

This project is partly funded by a grant from Information Technology Research Agency (ITRA), Department of Electronics and Information Technology (DeitY), Govt. of India.

REFERENCES

[1] Jiwen Cai; Ping Yi; Jialin Chen; Zhiyang Wang; Ning Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, "2010 24th IEEE International Conference on Advanced Information Networking and Applications", April 2010

[2] Ab-Hamid, K.; Chong Eng Tan; Sei Ping Lau, "Self-sustainable energy efficient long range WiFi network for rural communities," GLOBECOM Workshops (GC Wkshps), 2011 IEEE, vol., no., pp.1050,1055, 5-9 Dec. 2011

[3] Panigrahi, D.; Raman, B., "TDMA Scheduling in Long-Distance WiFi Networks," INFOCOM 2009, IEEE , vol., no., pp.2931,2935, 19-25 April 2009

[4] Sheth, A.; Nedevschi, S.; Patra, R.; Surana, S.; Brewer, E.; Subramanian, L., "Packet Loss Characterization in WiFi-Based Long Distance Networks," INFOCOM 2007, 26th IEEE International Conference on Computer Communications, IEEE, pp.312, 320, 6-12 2007

[5] Rabin Patra, Sergiu Nedevschi, Sonesh Surana, Anmol Sheth, Lakshminarayanan Subramanian, Eric Brewer, "WiLDNet: Design and Implementation of High Performance WiFi Based Long Distance Networks", 4th USENIX Symposium on Networked Systems Design & Implementation, 2007

[6] IETF MANET work group. http://www.ietf.org/dyn/wg/charter/ manetcharter.html

[7] Saloni Sharma, Anuj Kumar Gupta "A Comprehensive Review of Security Issues in Manets", International Journal of Computer Applications (0975 – 8887) Volume 69– No.21, May 2013

[8] L.D. Zhou; Z.J. Haas, Securing Ad Hoc Networks[J], IEEE Network, 13(6), 1999.

[9] K. Muthukumaran, D. Jeyakumar, C. U.Omkumar "A Concise Evaluation of Issues and Challenges in MANET Security", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 9, September 2013

[10] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013

[11] Hariom Soni, Preeti Verma "A Survey of Performance based Secure Routing Protocols in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 1, January 2013

[12] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah "A Survey on MANET Intrusion Detection", International Journal of Computer Science and Security, Volume (2): Issue (1), February 2008

[13] B.Praveen Kumar, P.Chandra Sekhar, N.Papanna and B.Bharath Bhushan "A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS", P Chandra Sekhar et al, Int.J.Computer Technology & Applications, Vol 4 (2), 248-256, 2013

[14] Manjeet Singh, Gaganpreet Kaur "A Surveys of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, 2013

[15] U. Sharmila Begam, Dr. G. Murugaboopathi "A RECENT SECURE INTRUSION DETECTION SYSTEM FOR MANETS", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, January 2013

[16] Mike Burmester, Breno de Medeiros, "On the Security of Route Discovery in MANETs" IEEE Transactions on Mobile Computing, vol. 8, no. 9, pp. 1180-1188, September 2009

[17] P.Visalakshi, S.Anjugam "Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey", International Journal of Computational Engineering Research, ISSN: 2250-3005 National Conference on Architecture, Software system and Green computing, 2013
[18] Sarvesh Tanwar, Prema K.V. "Threats & Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol.2, 2013
[19] Mohammad Wahid, Rajesh Kumar Singh and R.H. Goudar "A Survey of Attacks happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques", International Conference on Computer Communication and Networks CSI-COMNET-2011
[20] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012
[21] J. Godwin Ponsam, Dr. R. Srinivasan "A Survey on MANET Security Challenges, Attacks and its Countermeasures", International Journal of Emerging Trends & Technology in Computer Science (IJETICS) Volume 3, Issue 1, January – February 2014
[22] Dr. M.S. Aswal, Paramjeet Rawat and Tarun Kumar "Threats and Vulnerabilities in Wireless Mesh Networks", International Journal of Recent Trends in Engineering, Vol 2, No.4, 2009

AUTHORS

Dhaneesh B Nair received his B.Tech degree in Electronics and Communication Engineering from Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India in July 2013. He is currently pursuing M.Tech in Wireless Networks and Applications from Amrita Vishwa Vidyapeetham, Kollam, Kerala, India.

Dhanesh Raj received M.Tech. in Wireless Networks and Applications from Amrita Vishwa Vidyapeetham, Kerala and B.E. degree in Electronics and Communication Engineering from Anna University, Chennai. Since then, he has been working as a Research Associate in Amrita Wireless Networks and Applications at Amrita Vishwa Vidyapeetham. His current research interests include Cellular Networks, Mobile Communications and TVWS.

Prof. **Sethuraman Rao** is an associate professor at Amrita Center for Wireless Networks and Applications, Amrita University, Kollam, Kerala, India. He holds a Masters degree in Computer Science and a Bachelor's degree in Mechanical Engineering from IIT Madras, India. He has over 20 years of international experience in the networking industry having held technical and management positions at Juniper Networks, Alcatel-Lucent and a few startups. His areas of interest include wired and wireless LANs, wireless security, software engineering and network management.