METAHEURISTIC BASED ENERGY AWARE MULTILAYERED ALGORITHM FOR WIRELESS NETWORKS

S Pradeep 1, Dr Yogesh Kumar Sharma 2

1 Research Scholar, Dept. of CSE, JJT University, Jhunjhunu, Rajasthan, India
2 Head of the Department and Associate Professor, Dept. of CSE, JJT University, Jhunjhunu, Rajasthan, India

ABSTRACT:
In wireless networks, the wireless sensor networks are traditionally susceptible and vulnerable towards energy loss and lifetime based dimensions. Assorted Algorithms are devised so far to escalate the lifetime and energy of the wireless nodes still this area is under research as the inherent resource consumption are quite complex. In this research manuscript, the nature inspired approach titled elephant herd optimization is used for the overall performance and efficiency of wireless networks is used and using this approach the energy factors in wireless sensor networks can be optimized to a huge extent. This algorithmic approach is quite novel and provides efficiency in multiple parameters including cost, complexity, turnaround time and overall performance.

Keywords: Energy Optimization, Elephant Herd Optimization, Nature Inspired Algorithm, Wireless Sensor Networks

[1] INTRODUCTION

Wireless Networks are traditionally susceptible from assorted attacks and vulnerabilities including DDoS, Jamming, Trapping, Sybil and many others. Malicious Node attacks are traditionally used to tamper the network infrastructure from assorted dimensions. Such attacks can be implemented on any type of network associated with wireless technologies. Differences between assorted wireless technologies are –
Figure 1 – Taxonomy of Wireless Technologies

<table>
<thead>
<tr>
<th>Key Feature and Aspect</th>
<th>WiMax Technology 802.16a</th>
<th>Wi-Fi Technology 802.11a/g</th>
<th>Wi-Fi Technology 802.11b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Protocol</td>
<td>Request and Grant</td>
<td>CSMA/CA</td>
<td>CSMA/CA</td>
</tr>
<tr>
<td>Primary and Key Application</td>
<td>Wireless Broadband</td>
<td>WLAN</td>
<td>WLAN</td>
</tr>
<tr>
<td>Frequency Band</td>
<td>2-11 GHz</td>
<td>2.4 GHz ISM (g)</td>
<td>2.4 G Hz</td>
</tr>
<tr>
<td>Bandwidth of Channel</td>
<td>Adjustable / Customizable 1.25 - 20 MHz</td>
<td>20 MHz</td>
<td>25 MHz</td>
</tr>
<tr>
<td>Duplex Status</td>
<td>Full Duplex</td>
<td>Half Duplex</td>
<td>Half Duplex</td>
</tr>
<tr>
<td>Radio Technology</td>
<td>OFDM</td>
<td>OFDM</td>
<td>Direct Sequence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Spread Spectrum</td>
</tr>
<tr>
<td>FEC</td>
<td>Convolution Code</td>
<td>Convolution Code</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Reed-Solomon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>3DES</td>
<td>RC4</td>
<td>RC4</td>
</tr>
<tr>
<td></td>
<td>AES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bandwidth Efficiency</td>
<td>Less than Equal to 5 bps/Hz</td>
<td>Less than Equal to 2.7 bps/Hz</td>
<td>Less than Equal to 0.44 bps/Hz</td>
</tr>
<tr>
<td>Modulation</td>
<td>BPSK, QPSK,</td>
<td>BPSK, QPSK,</td>
<td>QPSK</td>
</tr>
</tbody>
</table>
Table 1 - Features and Related Dimensions of WiMax and WiFi Technologies

<table>
<thead>
<tr>
<th>Feature</th>
<th>WiMax</th>
<th>WiFi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility</td>
<td>Mobile WiMax</td>
<td>Under development</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Under development</td>
</tr>
<tr>
<td>Mesh Support</td>
<td>Present</td>
<td>Proprietary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proprietary</td>
</tr>
</tbody>
</table>

1.2 Energy Based Threats

The key threats to Wireless based on energy are hereby summarized:
- Non Optimal Path or Byzantine Allocation Attack
- Interception or Eavesdropping
- Jamming
- Modification or Black hole attack
- Rushing Malware Attack
- Wormhole or False Gateway Attack


Malicious Wireless Environment Node attack refers to the utilization of authentic node with data packet in the network by malicious node that causes tremendous utilization by the system prompting moderate exhaustion of node's battery life. By this way, the node’s battery is consumed to a huge extent by the malicious or attacker node so that the genuine node cannot communicate in the network. Such attack can damage the entire network as different nodes can be destroyed by making the life time of nodes’ battery to dead state.
One of the vital parts of Malicious Wireless Mote Attack is that it is convention free. It implies the Malicious Wireless Mote assaults can work and harm of any kind of system.

**FEATURES**

- Malicious Wireless Mote attacks are not specific to any protocol or topology or port.
- Malicious Wireless Mote Attacks do not interrupt the services directly. It affects the resources using the services.
- Malicious Wireless Motes makes use of protocol compatible or compliant messages
- Malicious Wireless Mote Attacks transmit data that drain the energy level of nodes.
- Malicious Wireless Motes do not change or interrupt altering discovered paths or routes.

Resource Draining Attacks – Such attacks create and send Malicious Wireless Mote attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node’s battery life.

The Malicious Wireless Mote attacks in the resource draining assaults can be classified has two types.

- Carousel attack
- Stretch attack.
Stateless Protocols

- These are Source Routing Protocols that keeps track of the communication in the network infrastructure.
- Source node specifies entire route to destination within packet header.
- Intermediaries don’t make independent forwarding decisions.
Stateful Protocols

- Nodes have advance information of state, topology, forwarding techniques and routes.
- Network Nodes create the local forwarding decisions on that stored state.

[3] Related Works and Literature Review

There are a few difficulties posture by the asset constraints in the remote sensor arranges because of the vulnerabilities that may happen because of element conduct of systems. Because of some of equipment imperatives the calculation must be surrounded with the parameters like transfer speed, computational multifaceted nature and memory. Since the expense happened is high when we compare correspondence as far as force, it may not be a unimportant assignment. So vitality effective remote sensor systems must be given at most need. The issue of security has gotten significant consideration via specialists in impromptu systems. Vulnerabilities in WSN could happen in light of specific measurements as per the qualities of element topology and absence of focal base station. There are a wide range of sorts of attacks that happen in remote impromptu sensor systems. There are preventive measures for these attacks in the MAC layer. A percentage of the strategies are underlined as under:

3.1 Path Based Attacks

These attacks are basic in remote wireless sensor systems. They are normally alluded as way based DoS (Denial of Service) attacks. Restricted hash chains can keep these attacks by constraining the rate at which hubs transmit parcels. In any case, one-way hash chains can't be utilized for a wide range of way based attacks. Particular techniques are utilized to wipe out particular sorts of path based attacks

3.2 Rushing Attack

Rushing attack occurs in on-interest directing conventions like DSR, Ad hoc On-Demand Distance Vector Routing (AODV) where course disclosure is finished by sending REQUEST messages to the neighboring hubs. In hurrying attack, the pernicious hub sends the REQUEST message much speedier when contrasted with the real hub. This outcomes in wrong course disclosure and the bundle is not sent to the destination. To keep this attack trust situated secured AODV convention is utilized where a trust edge worth is consolidated on the making trouble hub and in view of the trust esteem, the acting up hub can be detached. Another strategy is to utilize Rushing Attack Prevention (RAP) convention.

3.3 Wormhole Attack

In wormhole attack, the vindictive hub builds a passage (way) to the destination in such a path, to the point that all the bundles from the source are exchanged by means of the assailant which can change substance of the bundle before sending it to the destination. To keep this attack,
Packet confining system is utilized. A chain is data added to the packet in order to confine the packet path.

A Packet rope is of two sorts: i) Geographical chain is in view of the separation and the position of the collector ii) Temporal rope is in light of the lifetime of the recipient.

3.4 Routing Infrastructure Attacks

Routing infrastructure concentrates on insignificant vitality steering, which intends to utilize negligible vitality to transmit and get parcels and by utilizing insignificant vitality ways to transmit bundles. However utilizing such plans may lessen the system network and lifetime of the system. To dodge such issues, a vitality mindful directing convention, which uses sub-ideal ways, was presented. Numerous steering ways are available where the convention picks one taking into account probabilistic qualities. For this situation, each steering way is given an opportunity to exchange bundles along these lines improving the system lifetime.

3.5 Asset Exhaustion Attacks

Resource consumption attacks concentrate on lessening the amount of assets utilized by hubs like battery force, stockpiling, memory and so forth therefore diminishing the general limit of the system. There are numerous sorts of attacks like merry go round attack, stretch attack, directional receiving wire attack, and malevolent revelation attack. Numerous systems, for example, free source steering, secure conventions or checking the way for any circles can be utilized to counteract such attacks. Numerous plans proposed in the writing manage the detection and/or avoidance from asset weariness attack for the most part limited to different levels of convention stack including Medium Access Control layer (MAC) and application layer. A next to no examination is done on the asset depleting attack steering layer.

[4]. IMPLEMENTATION, RESULTS AND DISCUSSION

We have simulated the different scenarios for implementation of Malicious Wireless Mote Attacks avoidance using GPS sensor locators and timestamp based key generation. It is found in the results that the overall integrity and reliability is improved and battery power consumption is huge.

<table>
<thead>
<tr>
<th>Number of Wireless Nodes</th>
<th>Existing Approach</th>
<th>Proposed Approach</th>
<th>Simulation Iterations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>94</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>91</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>89</td>
<td>80</td>
</tr>
</tbody>
</table>

Table 2 - Energy Consume in the Classical and Proposed Approach
CONCLUSION AND SCOPE OF FUTURE WORK

In the proposed work to avoid and dettract the Malicious Wireless Mote attacks, an effective location based identifier is integrated in the network that will generate a dynamic key based on the GPS location and current timestamp. The generated hash key shall be matched in the source and destination channel and it will lead the transmission. Using this approach, the genuine packets shall not be lost. In case there packet loss, it is associated with the malicious node because in the algorithmic approach, the malicious node that is communicating with the data packet, then the data packet shall be dropped to avoid the security issues and improvement in the integrity. In the simulation scenario, the overall integrity and reliability of the network is improved using the proposed algorithm. The proposed algorithm can be integrated with Ant Colony Optimization that is one of the famous metaheuristic techniques for solving the combinatorial optimization problem. Using this technique, the dropped packet can be taken by the adjacent nodes (ants) then can it can be handed over to the destination.
REFERENCES


