A Fuzzy Approach to Avoid Selective Forwarding Attacks and Energy Efficient Path Selection in Wireless Mesh Networks

Er. Amandeep Singh¹, Er. Balraj Singh Sidhu², Dr. Jyoti Saxena³
¹,²,³Department of Electronics Engineering, GZS PTU Campus, Bathinda, INDIA

ABSTRACT

Wireless Mesh Networks (WMNs) have emerged as a key technology which provide support for next generation wireless networking and provide services that are not assisted by other Wireless Network. WMNs are deployed in an adverse environment. Due to which various types of security attacks can occur in WMNs such as wormhole, acknowledgement spoofing, black hole attack, sybil etc. So security plays an important role in WMNs. In this paper we study selective forwarding attack, how it affect the performance of WMNs and provide a Fuzzy based algorithm to protect WMNs against selective forwarding attack and provide a energy efficient path from transmitter to receiver. The performance is evaluated in terms of throughput, packet delivery ratio and average end to end delay. Simulation results have been provided to illustrate the efficiency of the proposed algorithm.


I. INTRODUCTION

Wireless Mesh Network (WMN) consists of a large number of nodes called mesh nodes and mesh routers which communicate through wireless medium and transmit information or data [8]. Data is transmitted in mesh network using a flooding technique or a routing technique. In flooding technique data is transmitted to all nodes so it is not an efficient way for data transmission. In routing technique, data is transmitted along a path, by hopping from node to node until the destination is reached. There is always more than one path are available between source and destination so routing play an important role in these networks. Packet switching is used in these networks and data is transmitted in the form of packets. A mesh network is known as fully connected network whose nodes are all connected to each other. Mesh networks are type of ad hoc network. Mobile ad hoc networks (MANET) and mesh networks are closely related to each other but MANET also have to deal with the problems caused due to the mobility of the nodes. WMNs are mostly deployed in hostile environment. So WMN are vulnerable to different attacks and selective forwarding attack is most severe of them [3].

Selective Forwarding Attack

In a forwarding attack malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.

In selective forwarding attack malicious nodes behaves like gray hole [7]. Node receives data from sender but do not forward the entire data and refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. It is difficult to detect the selective forwarding attack because neighboring nodes will conclude that data drop age is due to channel loss, heavy traffic and other losses present in the network. So selective forwarding attack is a more subtle form of black hole attack. An adversary can block or modifying packets originated or received from a few selected nodes in the network and can reliably transmit the remaining traffic [6]. In this way it limits suspicion of wrongdoing.

In figure 1 node "2" is working as attacker. If node "0" wants to send data it will forward data to node "2". Node "2" will drop some data and forward the remaining so node "2" is working as selective forwarding attacker.

Figure 1: Selective forwarding attack
In [1] C. Karlof and D. Wagner first time discussed the selective forwarding attack and suggested Multi-path routing to counter these types of attacks. If there are n paths in network then messages routed over n paths whose nodes are completely disjoint and network is completely protected against selective forwarding attacks. If a node is compromised then message can reach to destination through other available paths. Allowing nodes to dynamically choose next hop can further reduce the chances of an adversary gaining complete control of a data flow. But there is no detection of malicious nodes and poor Security Resilience if there exists at least one node in the path. Further there is increase in energy consumption and communication overheads.

In [2] Yu and Xiao proposed a distributed multi-hop acknowledgment scheme which detects selective forwarding attacks in both directions from base station and source node. This is based to launch alarms by obtaining responses from intermediate nodes. The detection process consists of upstream detection and downstream detection and uses three types of packets known as report packet, ACK packet and alarm packet. Downstream denotes direction towards base station and upstream denotes direction towards source node. The intermediate node after forwarding packet waits for ACK packet. When an intermediate node detects the misbehavior it forwards a report packet to base station through multi hops. Based on ACK packet received, source node identifies malicious node. The nodes can use multi-hop response acknowledgements in order to detect selective forwarding attack, resulting in certain delay and communication overhead. This scheme takes much effort to detect the selective forwarding attack.

In [3] Zhan, Xiong, Wang and Xin proposed a distributed light weight defense scheme against selective forwarding attack. In this approach neighbor nodes are used to find misbehavior. Here they used a hexagonal mesh topology. This scheme utilizes the neighbor nodes to monitor the transmissions of the event packet and detect selective forwarding attack by monitoring packets forwarding of two nodes in the transmission path and resend these packets dropped by the attackers to the destination node. The monitor node is responsible for the detection of possible selective forwarding attack and if selective forwarding attack is identified, it retransmits the event packet to the destination node and finally when selective forwarding attack is detected, it sends an alarming message to its neighbor nodes for notifying the location of attacker thus avoiding the attacker node in forwarding of incoming packets. The authors have made some assumptions that network location does not change after deployment and efficiency of scheme decreases if network topology changes.

In [4] Xiao and B.Yu proposed a scheme to identify attacker nodes in selective forwarding attack known as checkpoint based multi-hop acknowledgement scheme (CHEMAS). Actually it is improvement of previous scheme for detection of selective forwarding attack. In this scheme randomly intermediate nodes are selected along a forwarding path called checkpoint nodes which are responsible for generation of acknowledgements for each received packet. Selection is made on a one-way hash key chain for ensuring the authenticity of packets. Each intermediate node in a forwarding path has the potential to detect abnormal packet loss and identify compromised nodes. There is problem of storage space for one-way hash key chains for authentication of each packet and more energy is consumed by sending acknowledgement.

In [5] Hea Young and Tae Ho C. have proposed an improved form of Multipath routing method using Fuzzy based reliable data delivery scheme for countering selective forwarding attack. Here the number of transmission path varies with number of attacker. The number of paths for data delivery is determined by a fuzzy logic with consideration of the energy level of the network and the number of malicious nodes. The proposed method uses the propagation limiting method as a means for routing if multi-path routing is insufficient for reliable data delivery. They have also assumed that the base station know or estimate the energy level of network and the number of compromised nodes in advance and all nodes in the network know their location which is difficult to determine. This scheme is not able to detect compromised nodes and there is also increase in communication overhead.
Chanatip T. and Ruttikorn V. [6] have proposed a Traffic Monitoring Based scheme to detect selective forwarding attacks. Their approach uses traffic analysis of the entire network. The authors have used Received Signal Strength Indicator (RSSI) value from monitoring nodes to determine the position of all nodes with the Base Station (BS). They have focused on an address based selective forwarding attack in which, the attacker selectively drops packets based on the source address. As a result, the attacker affects Denial of Service Attacks (DOS) for those nodes only, while remaining normal for all the other nodes. The authors have made assumptions that the network is static, where all nodes are immobile after initial deployment. So scheme fails when topology of system is changed. They have assumed that the BS and monitoring nodes are physically protected which is practically not possible.

Devu Manikantan Shila and Tricha Anjali [7] proposed a Threshold Based technique against selective forwarding attack. This scheme can detect the malicious nodes quickly and additional overhead caused by the algorithm also minimum. AODV protocol determines the path between source and destination nodes. Each node maintains a packet counter for keeping track of the packets received from a particular source node. The source node also maintains a packet counter to keep track of the packets forwarded to destination node. In this detection scheme two packets, Control packet and Control ACK are used. When the destination node receives the Control packet, it retrieves the packet count value in Control packet. The destination node compares the destination packet count with the detection threshold and returns an acknowledgment (Control ACK) for every received Control packet. A positive Control ACK will be sent to the source node if the destination packet count satisfies the detection threshold to notifying the absence of attacker in the forwarding path. Otherwise a negative Control ACK will be sent to the source node. A Timeout is used when no Control ACK is received. After the Timeout, source node will initiate the Query based localization algorithm. The accuracy of the detection of malicious node depends upon detection threshold calculation. This scheme provides less efficiency due to hard decision threshold.

In previous work we set three thresholds levels high, medium and low based on single variable which define the dropped packets between nodes. But this time we used multiple variables or levels to define these thresholds levels. Multiple levels provide an efficient way to calculate the final value of path loss rate which is very close to the actual value. The performance of each node is evaluated in the network from source to destination. Medium and low levels define that the network is good for communication and high level defines a weak link. Each level indicates different loss rates through the use of priorities.

When it is conformed that no adversary is present in the network then we check for false alarms and optimum path from source to destination because in mesh network there is always more than path present between source and destination nodes. In this step each node which acts as router is tested for conditions which provide the best results. In order to identify the best neighbor node we check the three parameters lost packets, expected rate and last packet time. Lost packets define the number of lost packets, expected rate defines the number of expected packets to be received at the receiver side and last packet time is used to calculate the time of last packet of stream received at the receiver side which indirectly includes the communication path delay. By using these three parameters we set the priorities. When lost packet is low, expected rate is high and last packet time is low conditions are better for data transmission and priority is high. When lost packet is medium, expected rate is medium and last packet time is medium then priority is medium. When lost packet is high, expected rate is low and last packet time is high then priority is low.

After observing these parameters we check the energy level. Energy level defines the amount of energy required by a particular node to transmit data. A node having low energy level can transmit the data to long distance using less energy. Because of less energy life of node is increased. So low energy level provides better conditions for communication. When all neighbor nodes are at same energy level then we examine the network for a node providing optimum communication. When a node is selected communication starts and same test is performed at each node through the transmission path.

II. SOLUTION METHODOLOGY

We proposed an algorithm to design an intrusion detection system to detect the forwarding attack on WMN by making use of two factors i.e. number of packets and forward packet delivery ratio on basis of delay, loss and expected data rate. This detection system is based on FUZZY LOGIC. Fuzzy Logic provides a definite conclusion based upon noisy or missing input information. The performance is evaluated in terms of throughput, packet delivery ratio and average end to end delay.

III. PROPOSED ALGORITHM

1. Construct a wireless network with n nodes in wxh network
2. Define the communication and energy parameters for each node
3. Define the source node Src, destination node dst and current node curNode
4. Include the attack over the network
5. Set CommThreshold
proc High { Factor }
{
    set a .5
    set b .8
    set c 1
    if { $Factor == $b } {
        set factor 1
    } elseif { $Factor >= $a && $Factor < $b } {
        set factor [expr ($Factor - $a) / ($b - $a)]
    } elseif { $Factor >= $b && $Factor <= $c } {
        set factor [expr ($c - $Factor) / ($c - $b)]
    } else {
        set factor 0
    }
    return factor;
}
proc Low { Factor }
{
    set a .3
    set b .5
    if { $Factor < $a } {
        set factor 1
    } elseif { $Factor >= $a && $Factor < $b } {
        set factor [expr ($b - $Factor) / ($b - $a)]
    } else {
        set factor 0
    }
    return factor;
}
proc Medium { Factor }
{
    set a .2
    set b .5
    set c .8
    if { $Factor == $b } {
        set factor 1
    } elseif { $Factor >= $a && $Factor < $b } {
        set factor [expr ($Factor - $a) / ($b - $a)]
    } elseif { $Factor >= $b && $Factor <= $c } {
        set factor [expr ($c - $Factor) / ($c - $b)]
    } else {
        set factor 0
    }
    return factor;
}

6. While curNod=Dst
   [Repeat steps 7 to 14]
7. Identify the neighboring nodes of curNode and maintain them in a list called Nlist
8. For i=1 to Length(NList)
   {
9. For j=1 to Length(NList)
   {
   [Repeat Steps 10 to 14]
10. Check data rates
11. Analyze
            energy=EnergyReq(Comm(curNode,NList(i)&&NList(j)))
12. If (data<CommThreshold and rate<RateThreshold and energy<EnergyThreshold)
   {
13. Transmit Data
   }
   Else
   {
14. Find Next neighbor for optimum transmission
   }
}

IV. PERFORMANCE EVALUATION

The proposed system is implemented in NS2 and system performance is evaluated in terms of throughput, packet delivery ratio and average end to end delay.

A. Simulation Parameters

The network topology consists of a square grid of 26 mesh nodes and 5 nodes working as attacker. In our simulations UDP and FTP are used for data transfers. AODV routing protocol is used for routing between source and destination. Packets have a size of 512 bytes and are sent at a deterministic rate.

B. Simulation Analysis

From table number 1 it is clear that there is significantly increase in the throughput and packet delivery ratio of the network. Results are also shown using graphs with respect to simulation time.

<table>
<thead>
<tr>
<th>Time(ms)</th>
<th>Throughput (Proposed approach)</th>
<th>Throughput (Exiting work)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>627.32</td>
<td>336.50</td>
</tr>
<tr>
<td>10</td>
<td>627.98</td>
<td>336.73</td>
</tr>
<tr>
<td>15</td>
<td>629.24</td>
<td>336.63</td>
</tr>
<tr>
<td>20</td>
<td>629.18</td>
<td>336.32</td>
</tr>
<tr>
<td>25</td>
<td>630.36</td>
<td>336.25</td>
</tr>
<tr>
<td>30</td>
<td>629.70</td>
<td>336.21</td>
</tr>
<tr>
<td>35</td>
<td>630.32</td>
<td>336.19</td>
</tr>
<tr>
<td>40</td>
<td>630.43</td>
<td>336.03</td>
</tr>
<tr>
<td>45</td>
<td>630.7</td>
<td>335.96</td>
</tr>
<tr>
<td>50</td>
<td>631</td>
<td>335.96</td>
</tr>
</tbody>
</table>
TABLE 2

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Packet delivery ratio (Proposed approach)</th>
<th>Packet delivery ratio (Existing work)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>98.99</td>
<td>7.31</td>
</tr>
<tr>
<td>10</td>
<td>97.5672</td>
<td>6.943</td>
</tr>
<tr>
<td>15</td>
<td>98.4477</td>
<td>6.82085</td>
</tr>
<tr>
<td>20</td>
<td>97.935</td>
<td>6.7516</td>
</tr>
<tr>
<td>25</td>
<td>98.3719</td>
<td>6.71016</td>
</tr>
<tr>
<td>30</td>
<td>98.4323</td>
<td>6.68781</td>
</tr>
<tr>
<td>35</td>
<td>98.3835</td>
<td>6.66941</td>
</tr>
<tr>
<td>40</td>
<td>98.5032</td>
<td>6.65174</td>
</tr>
<tr>
<td>45</td>
<td>98.424</td>
<td>6.643</td>
</tr>
<tr>
<td>50</td>
<td>98.4944</td>
<td>6.63489</td>
</tr>
</tbody>
</table>

Figure 5: Packet Delivery Ratio versus Simulation Time

But there is increase in the average end to end delay which is caused by the increase in the complexity of nodes. This average end to end delay can be decreased by increasing the system bandwidth due to which system become expensive. But average end to end delay remains almost with the increase in the hop count of the nodes which is the biggest advantage of proposed system. By calculating the average end to end delay in advance we can select the appropriate bandwidth to reduce average end to end delay.

V. CONCLUSION

In this paper we proposed a Fuzzy based algorithm using multiple levels at every threshold level which would defend against the selective forwarding attack and this is based on the prioritization approach so that always the less critical node will be selected as the participating node. Further more energy efficient node is selected which can transmit the same amount of data by using less energy. The scheme has been evaluated using the simulator NS-2 and results are compared with previous work which shows a significant increase in throughput. But there is increase in
average end to end delay but it remains almost constant with increase in hop count. Thus the system has successfully defended the attack and provides a reliable data transmission. Further performance can be improved by using protocols such as DSR etc.

REFERENCES


