Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Fuzzy Logic Approach to Detect and Avoid Selective Forwarding Attacks in Wireless Mesh Networks

Amandeep Singh, Er. Balraj Singh Sidhu, Dr. Jyoti Saxena

Deptt. of Electronics Engg.
GZS PTU Campus, Bathinda , India

Abstract— In recent days, Wireless Mesh Networks (WMNs) are emerging as an interesting area. WMNs provide technology for next generation wireless networking to provide services that are not supported by other Wireless Network. WMNs are mostly deployed in hostile environment where these are unattended. So WMNs are vulnerable to different types of security attacks such as wormhole, black hole attack, sybil etc. So security is major concern in WMNs. In this paper most serious attack known as selective forwarding attack is investigated. In this attack a malicious node drops all or some of received packets. An algorithm is defined to protect WMNs against selective forwarding attack which is based on Fuzzy Logic. Fuzzy Logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, impressive, noisy or missing input information. The performance is evaluated in terms of throughput and average end to end delay. Simulation results have been provided to illustrate the efficiency of the proposed algorithm.

Index terms— Wireless Mesh networks, Selective forwarding attacks, Route Reply Packet, Fuzzy Logic, Detection threshold.

I. INTRODUCTION

Wireless Mesh Network (WMN) is the most effective technology used in third generation wireless networking. WMN consists of a large number of nodes called mesh nodes and mesh routers which communicate through wireless medium and transmit information or data. The number of nodes in a network can vary from hundreds to thousands. The mesh nodes are stationary and mesh routers form backbone of the network. Packet switching is used in these networks and data is transmitted in the form of packets. There are always more than one data paths or routes are available between the sender and the receiver. Hence routing plays an important role in the entire network. To support end to end communication routing protocols are required. Mesh networks may involve either fixed or mobile devices. WMN networks are used in diverse communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance etc. An important possible application for wireless mesh networks is voice over Internet Protocol (VoIP). By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh. So WMNs are mostly deployed in such situation where it is possible for the adversary or attacker to take control of one or more nodes of the network. Due to this WMNs are vulnerable to various types of attacks and selective forwarding attack is most difficult to detect from them.

]A. Selective Forwarding Attack

Forwarding attack is one of many possible attacks in WMN. In this attack, a malicious node sends a forged Route Reply packet (RREP) to a source node that initiates the route discovery in order to pretend to be a destination node. When a source node received multiple RREP then by comparing the destination sequence number (defines an up-to-date path to a destination) contained in each RREP packets it finds the greatest one as the most recent routing information and selects the route contained in that RREP packet. In case the sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker. Therefore, source and destination nodes become unable to communicate with each other.

A forwarding node can also send a reply to a route request (RREQ) message from any source in the network which shows the node itself is a nearest node to the destination and receive all the packet of data meant for some other node from the source node.

In forwarding attack malicious node behaves like black hole or the gray hole. In black hole attack malicious node refuses to forward all packets and simply drops them, ensuring that they are not propagated any further. However, such an attacker runs the risks that neighboring nodes will conclude that attacker node has failed and decide to seek another route. A more subtle form of this attack is gray hole attack in which a malicious node selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic and reduces suspicion of wrongdoing because some packets are also dropped due to channel losses and increased congestion with increase of traffic. In such scenario it becomes very difficult to find an attacker in the WMN networks.

B. How Forwarding affects WMNs

In figure1 it is shown that in Ad Hoc On-Demand Distance Vector (AODV) routing network the malicious node “A” first detects the active route in between the sender “E” and destination node “B”. The malicious node “A” then send the RREP to node "C" which contains the spoofed destination address of node "B" including small hop count and large sequence number. Then node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the malicious node "A" instead of correct node "B". When malicious node "A" receives data from node "C" it will drop some data and remaining data will be sent to destination node "B". In this way sender and destination node will be in no position to communicate accurately in state of selective forwarding attack. This type of attack mostly takes place in border area, where it becomes difficult to detect enemy movement across the border and a country can also loss a war.

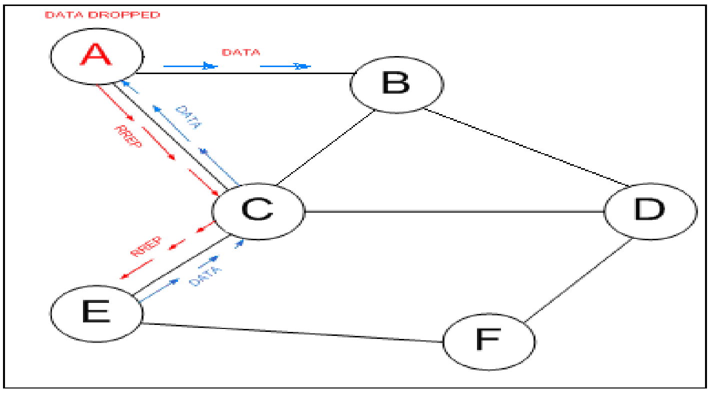

Fig. 1 Selective forwarding attack specification

In [1] Shekhar Tandan and Praneet Saurabh (2011) proposed a packet drop ratio (PDR) based detection technique for blackhole attack in mobile adhoc networks (MANET). It is a Threshold detection technique in which calculated packet drop ratio (PDR) is compared against a Threshold value. Threshold value is a maximum packet drop ratio value without blackhole attack. Under the normal case i.e. without attack, Packet Drop Ratio (PDR) must always be less or equals to threshold value. Under attack case packet drop ratio will be more than the threshold value. But this algorithm provides no solution for selective forwarding attack.

In [2] C. Karlof and D. Wagner (2003) suggested Multi-path routing to counter selective forwarding attacks. They proposed n paths in network then messages routed over these n paths whose nodes are completely disjoint and in this way network is completely protected against selective forwarding attacks. If a node is compromised then message can reach to destination through other available paths. But in this mechanism no solution is provided to find malicious node and also problem of heavy traffic.

In [3] Wang Xin-sheng et. al (Oct.2009) proposed a distributed light weight defense scheme against selective forwarding attack. In this approach neighbor nodes of attacker node are used to locate misbehavior. Here a hexagonal mesh topology has been proposed. This scheme utilizes the neighbor nodes to monitor the transmissions packet and detect selective forwarding attack by monitoring packets forwarded by two nodes in the transmission path. After locating the malicious node the source node resend these packets dropped by the attackers to the destination node. There is no mechanism provided to count channel losses.

In [4] H. Sun, C. Chen and Y. Hsiao (Oct.2007) have proposed multi dataflow topologies against selective forwarding attack. In multi dataflow scheme, the whole network is divided into different data topologies and one packet is sent through two topologies. Through two topologies the base station can defend against the selective forwarding attack. If a malicious node exists in one topology, the base station can still obtain packets from other topology. This scheme does not provide efficient solution.

In [5] J. Brown and X. Du (May 2008) proposed an efficient centralized cluster based scheme to detect selective forwarding using a Heterogeneous Sensor Network (HSN) model. The scheme uses a Sequential Probability Ratio Test (SPRT) method. For each node, probability value ’p’ is calculated which is equal to the percentage of dropped packets in all forwarded packets at a node. The scheme considers three threshold value p_0, p_1 and p_2.If node has a value of p less than p_1 then it is considered as legitimate node and if value is p is greater than p_1 then it is considered as a compromised node. But no mechanism is provided for retransmission of dropped packets.

In [6] B. Yu and B. Xiao (2007) have proposed a technique for identifying suspect nodes in selective forwarding attack called checkpoint-based multi-hop acknowledgement scheme (CHEMAS). Actually it is improvement of their previous technique for detection of selective forwarding attack. In this scheme randomly an intermediate nodes is selected along path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. Each intermediate node has the potential to detect abnormal packet loss and identify compromised nodes. There is no guarantee for reliable data transmission.

In [7] Devu Manikantan Shila and Tricha Anjali (May 2008) proposed a reliable Threshold Based Technique against selective forwarding attack. This scheme can detect the malicious nodes quickly and additional overheads caused by this algorithm are also minimum. Each node maintains a packet counter for keeping track of the packets received from a particular source 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 from 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 is greater than or equal to detection threshold which indicate the absence of attacker in the forwarding path. Otherwise a negative Control ACK will be sent to the source node.

II. SOLUTION METHODOLOGY

We proposed an algorithm to design an intrusion detection system to detect the forwarding attack in WMNs by making use of two factors i.e. no 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 and average end to end delay.

First we set three thresholds levels high, medium and low which define the dropped packets between nodes. These dropped packets include the loss rate due to the channel losses and increased traffic in the network. 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 condition to get 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 no of lost packets, expected rate defines the no 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 indicates the delay of the communication path. 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. A node having optimum conditions is selected and communication starts. Same test is performed at each node through the transmission path.

III. PROPOSED ALGORITHM

1. Construct a wireless network with n nodes in wxb network
2. Define the communication and energy parameters for each node
3. Define the source node Src, destination node dst and current node cur
4. Include the attack over the network
5. Set CommThreshold

```
High { Factor }
{
set c 1
      if { $Factor ==$c }
{
        set factor 1
}
              else
{
          set factor 0
              }

return factor;
}

Low { Factor }
{
set a .3
      if { $Factor < $a }
{
        set factor 1
              }
else
{
          set factor 0
              }

return factor;
}
Medium { Factor }
{
set b .5
        if { $Factor == $b }
 {
          set factor 1
                 }
else
{
            set factor 0
                 }

return factor;
}
```

```
    6.  While curNod=Dst
        [Repeat steps 7 to 12]
    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 8 to 12]
    10. Analyze data and  rate

    11. If (data<CommThreshold and rate<RateThreshold)
        {
    12. Transmit Data
        }
    Else
        {
    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 and average end to end delay.

A. Simulation Parameters

The network topology consists of a square grid of 26 mesh nodes. 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 no.1 it is clear that there is significantly increase in the throughput of the network. Results are also shown using graphs with respect to simulation time.

TABLE 1
THROUGHPUT

Time (ms)	**Throughput1 Using Fuzzy Logic Approach**	**Throughput2 Using Threshold Technique**
5	96	89
10	118	96
15	189	116
20	89	40
25	69	36
30	149	65
35	139	45
40	189	75
45	204	90
50	176	112

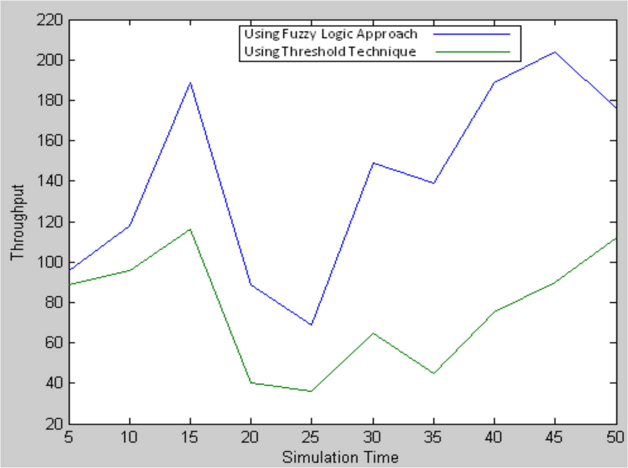

Fig. 2 Throughput versus Simulation Time

TABLE 2
AVERAGE END TO END DELAY

Time(ms	Average end to end delay1 Using Fuzzy Logic Approach	Average end to end delay2 Using Threshold Technique
5	55.44	3.5
10	45.0095	3.5
15	47.5184	3.5
20	47.36	3.5
25	43.95	3.5
30	44.3099	3.5
35	45.6544	3.5
40	46.6133	3.5
45	44.136	3.5
50	44.0588	3.5

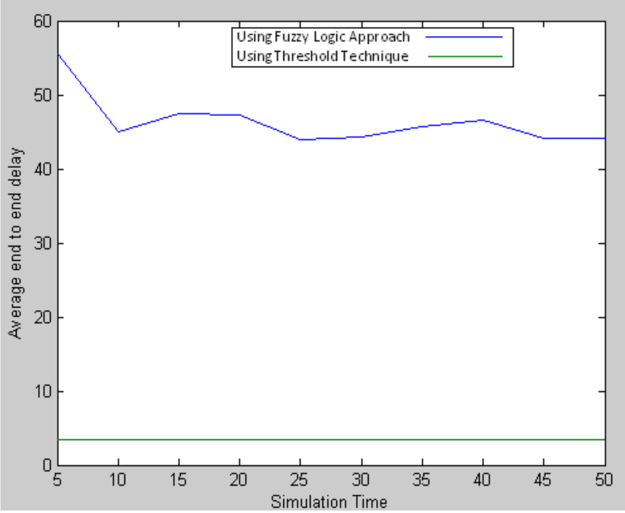

Fig. 3 Average End To End Delay versus Simulation Time

But there is increase in the average end to end delay which is caused by the increase in the complexity of nodes and increased amount of overhead in the network. This average end to end delay can be decreased by increasing the system bandwidth due to which system become expensive. By estimating average end to end delay in advance we can select the appropriate system bandwidth which will provide optimum and reliable data delivery.

V. CONCLUSION

In this paper we proposed an algorithm based on Fuzzy Logic which would defend the network from the selective forwarding attack and this is based on the prioritization approach so that always the less critical nodes will be selected as the participating node. Proposed system provides a better throughput in hostile environment. Simulation results are used to illustrate the efficiency of the proposed system**.** The scheme has been evaluated using the simulator NS-2 and results are compared which show a significant increase in throughput. But there is increase in average end to end delay whose affect can be reduced by increasing the system bandwidth. Thus, the system has successfully defended the attack and provides a reliable transmission. Further performance can be improved by selecting the energy effective route in case of AODV protocol so that network life will be increased.

REFERENCES

[1] Shekhar Tandan and Praneet Saurabh (2011), *A PDRR based detection technique for blackhole attack in MANET*, International Journal of Computer Science and Information Technologies, Vol. 2 (4), pp 1513-1516.

[2] C. Karlof and D. Wagner (2003), *Secure routing in wireless sensor networks: attacks and countermeasures*, IEEE International Workshop, ISBN 0-7803-7879-2, pp 113 - 127.

[3] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming and Wang Liangmin (Oct.2009), *Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Network*', Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC '09. International Conference, ISBN 978-1-4244-5218-7, pp 226 –232.

[4] H. Sun, C. Chen and Y. Hsiao (Oct.2007), *An efficient countermeasure to the selective forwarding attack in wireless sensor networks*, in Proc of IEEE TENCON 2007, ISBN 978-1-4244-1272-3, pp 1-4.

[5] J. Brown and X. Du (May 2008), *Detection of selective forwarding attacks in heterogeneous sensor networks*, in International Conf. on Communications, ISBN 978-1-4244-2075-9, pp 1583-1587.

[6] B. Yu and B. Xiao(2007), *CHEMAS: identify suspect nodes in selective forwarding attacks*, in Journal of Parallel and Distributed Computing, Vol. 67, No. 11, pp 1218-1230.

[7] Devu Manikantan Shila and Tricha Anjali(May 2008), *Defending Selective Forwarding Attacks in WMNs*, in Electro/Information Technology, 2008. EIT 2008. IEEE International Conference, ISBN 978-1-4244-2029-2, pp 96 - 101.

[8} F. Akyildiz, Xudong WANG and Kiyon(Sept. 2005), *A survay on Wireless Mesh Network WMNs*, Communications Magazine, IEEE ,Volume:43 , Issue: 9, pp S23 - S30.

[9] I.D. Chakeres and E.M.B.-Royer(March 2004), *AODV Routing Protocol Implementation Design*, in Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN), Tokyo, Japan, ISBN 0-7695-2087-1, pp 698-703.

[10] Jani Hautakorpi, *IEEE 802.11 and wireless simulations in ns2*, Ns notes and documentation.