International Journal of Engineering & Technology, 7 (3.29) (2018) 301-303

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Simulation analysis on network layer attacks in wireless mesh networks

K. Ganesh Reddy [1] *, M. S. Sudheer [1], P. Kiran Sree [1], V. Purushothama Raju [1]

[1] Department of CSE, SVECW, Bhimavaram, India
**Corresponding author E-mail: Guncity11@gmail.com*

Abstract

Security mechanisms in Wireless Mesh Networks (WMNs) play an essential role to protect WMNs features. However, the existing security standards of WMNs are still in draft state. In addition to that, WMNs features like integrating with heterogeneous nodes and networks, which make designing robust security mechanism for WMNs is more complex. To develop an efficient security mechanism for WMNs, firstly we need to study the vulnerabilities of WMNs, and then exploit these vulnerabilities to perform various attacks and find the counter measures for these attacks. In this paper, we have studied various network layer attacks, based on this study we identified the interdependencies of these attacks. We use AODV protocol to exploit these attacks. Our simulation results show that the each attack severity with respect to goodput and Packet Delivery Ratio (PDR). We explained how these severity measures are useful for future WMNs security mechanisms.

Keywords: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

1. Introduction

In recent years, WMNs have become more popular because of its ubiquitous broadband wireless internet connectivity in a sizable geographic area and cost effective network deployment. WMNs have ad-hoc features such as self-organizing, self-configuring, self-healing etc. They can interoperate with other wireless networks such as high-speed metropolitan area mobile networks, and have backhaul connectivity for cellular radio access networks, intelligent transport system, network defense system, citywide surveillance systems etc. In contrast, specific wireless networks such as cellular, ad-hoc, and sensor networks do not support most of the mesh features like high bandwidth, scalability, and interoperability with heterogeneous networks[1,2,3,6,8]. Due to emerging applications of WMNs, research groups have developed new standards such as 802.11s, 802.16 (Wi-MAX), and 802.20 [1], [10 - 14]. However, these standards were developed with limited features of WMN architecture, for example, 802.11s and 802.16 do not support the multi-hop client mesh topology, distributed authentication, authorization, and accounting (AAA) servers authentication etc. The limitations of WMNs existing standards, restrict the scalability of the network. Moreover, security protocols of these standards are still in draft stage, as these standards adopted security protocols from other wireless networks such as ad-hoc networks, sensor networks, and cellular networks etc [5], [7], [9]. Compatibility and integration are the major issues when WMNs adopted these security protocols, and this creates new vulnerabilities in WMN. Due to inadequate secure protocols, wireless mesh networks are more vulnerable especially in three layers: Network layer, MAC layer and Physical layer [4], [13], [15].Out of which, network layer security is more vulnerable due to dynamic topology and self-organized multihop routing. These network layer vulnerabilities lead to various network layer attacks. We have implemented network layer attacks in ns2 to find the severity of network layer attacks. Our simulation shows that, out of all attacks wormhole and location discloser related attackers severely degrade the network performance. Based on the simulation results we relate severity of the attack is equal to reputation value of the attack.

The rest of the sections as follows, section 2, describes study of various attacks in network layer, section 3 relates the attacks dependencies, section 4 shows the simulation results and section 5 concludes this paper.

2. Study of various attacks in network layer

In this section, we have studied blackhole attack, grayhole attack ,rushing attack, wormhole attack and location discloser attack.

Blackhole attack: In this attack, adversary node drops all the packets passed through it. In order to do this, the adversary node attracts the neighbor node with false route reply with less hop count and greater sequence number. Once, route is established through that node then the source node starts sending packets to the destination node. Eventually, all packets will be dropped at adversary node. Many wireless routing protocols such as AODV, DSR, HWMP, DSDV etc. are vulnerable to Blackhole attack.

Grayhole attack: Adversary node uses same idea of blackhole attack to participate in the active route. Once, route is established through the adversary node for packet forwarding, it selectively drops the packets, instead of dropping all the received packets. Detecting grayhole attack is more complex than blackhole attack.

Rushing attack: Rushing attack is a zero delay attack and more effective when the attacker nearby source or destination node. On-demand routing protocols like AODV and DSR are more vulnerable to this attack, because whenever source node floods the route request packet in the network, an adversary node receives the route request packet and sends without any hop_count update and delay in to the network. Whenever the legitimate nodes receive the

original source request packets, they are dropped because legitimate nodes, would have already received packet from the attacker and treat the currently received packets as duplicate packets. Thus, adversary is included in active route and disturbs the data forwarding phase. Rushing attack can be taken place at source side or destination side or at the middle.

The following conditions the rushing attacker is not included in active route

1) When source and destination nodes have direct communication link
2) When source and destination nodes have better route than rushing attackers' route

Rushing attack is more effective when attacker near to source or destination node

Wormhole attack: Less communication delay and more coverage area are the two important characteristics for forming effective route in wireless network. If the nodes have these characteristics, most often those nodes are in the active route as compared to the conventional nodes. Malicious nodes use these two false characteristics to participate in the active route, we also called this type of attack as wormhole attack. Usually, two or more colluding attackers' create wormhole attack, and to do this attack colluding attackers' form malicious tunnels with less delay and more coverage area. Once attackers are in the active route, all these attackers receive network traffic from their neighbouring nodes to forward this traffic to corresponding destination.

Location Discloser attack: In this attack, malicious node will fix the targeted node in the network and create Denial of Service (DoS) attack by flooding fake packets. It causes buffer overflow problem at targeted node. Any internal node in the network can acts as malicious node because all the nodes know the network topology. This attack can also be performed by external attackers when the attacker has topology information otherwise it uses brute force mechanism to find the targeted node location.

Jellyfish attack: In this attack, malicious node receives the packets from its neighbouring nodes then it intentionally increases the data packets delay before forwarding the packet to the next node. This attack is more severe because of the network throughput can be degraded to zero.

Byzantine attack: In byzantine attack, a malicious intermediate node or a set of malicious intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behaviour.

3. Attacks interdependencies

Based on this network layer attacks, we derive the interdependency of control plane attacks such as Black hole, Grayhole , Rushing, Wormhole, and location discloser attacks and data plane attacks such as jellyfish and Byzantine attacks. In control plane, attackers attracts the network nodes by sending less hop count, delay, multiple address, and long coverage area to join in active route. Once attacker is on active route then it start doing data plane attacks. We have defined the interdependency of attacks in the following:

Location discloser attack-> control plane flooding, fake data packets flooding traffic pattern distortion

Wormhole attack-> Jellyfish and Byzantine attacks

Rushing attack-> Jellyfish and Byzantine attacks

Gray hole attack-> Byzantine attack

Black hole attack-> Byzantine attack

The above attacks interdependencies are implemented in network simulator (ns), to identify the severity of the attacks.

4. Simulation of detection solution

To evaluate the severity of the attacks we used the same scenarios and simulation parameters. Conventional AODV protocol doesn't provide any security related to control plane and data plane attacks. We have created malicious nodes Black hole, Grayhole , Rushing, Wormhole, and location discloser attacks. These nodes have high probability to be in the active path of AODV protocol.

Table 1: Simulation Parameters

Parameter	Value
Number Of Nodes	40
Simulation Time	1000sec
Routing Protocol	Aodv
Queue Type	Drop Tail
Packet Size	1500 Bytes
Transport Protocol	Udp
Network Size	2000mx2000m
Percentage Of Malicious Node	10-20
Node Mobility	Random Mobility

We have chosen 10 to 20 percentages of malicious nodes in the network also called attack scenario. To perform the blackhole attack, first these malicious nodes send false replay(less hop_count) upon receiving the route request, second, all the received data packets are dropped by these malicious nodes. To perform grayhole attack, malicious nodes only drops the selective packets in random time intervals. To perform the rushing attack, malicious nodes immediately broadcast the request packet without processing upon receiving the route request. To perform the wormhole attack, malicious nodes uses more radio ranges then the other network nodes. Both rushing and wormhole malicious nodes intentionally increase packets delay and the drop the data packets. To perform location discloser attack, malicious nodes find the targeted node by using random mobility concept, once it finds targets node malicious node floods fake request packets.

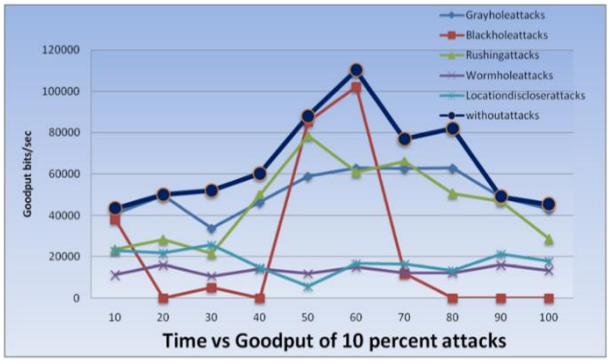

Fig. 1: Goodput Over 10% Attack Scenarios.

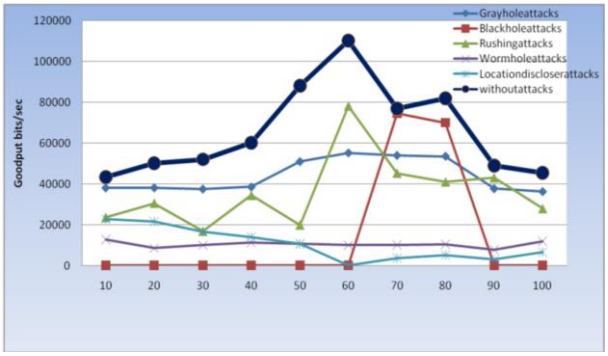

Fig. 2: Goodput Over 10% Attack Scenarios.

We apply the random mobility for all the nodes in the 2000mX2000m geographical area, shown in Table 1. If no attacks exist in the network (non attack scenario), every node has equal chances to be in the active route.

We have compared the attack scenarios and non attack scenario with respect goodput and time. Initially, 10% of attacks are present in the network and we have observed following results:

Blackhole attack scenario goodput often touch to zero and some time it near to non attack scenario goodput, this because attacker may not present in the active path. Grayhole attacks goodput do not degrade much like other attacks because attacker drops only selective packets as shown in Figure 1 and 2. Rushing attacks have less chance to participate in active route due to node mobility. Moreover, rushing attacks are effective only when attacker is near to source or destination, this is not always possible. Hence, goodput does not affect much like other attacks. Location discloser attacks, attacker tries to identify the target node here we consider target node as a destination node, once the attacker identify the target node it start flooding by control packets or fake data packets. In this attack throughput degrades severely then previous attacks. Wormhole attacks are very severe attacks than any other attacks. Here, the attackers attract the networks node by sending false details like less delay and broad coverage area. These two factors attract neighbours to send their data through wormhole malicious nodes. Goodput of the wormhole attack is not more than 12-18kbps means 85-90 percent of goodput is debilitated.

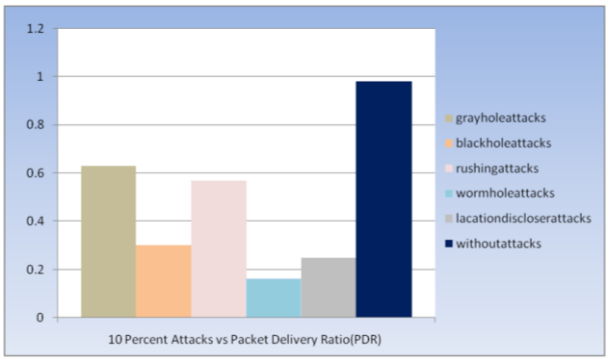

Fig. 3: Packet Delivery Ratio Over 10% Attack Scenarios.

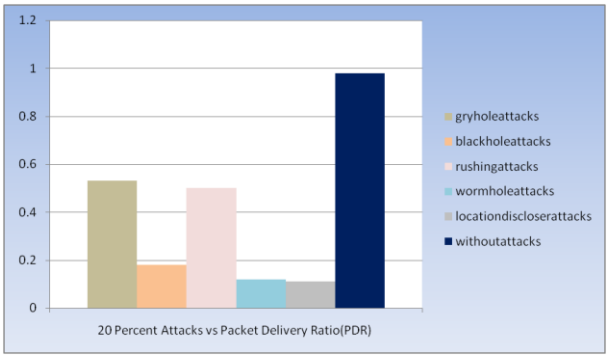

Fig. 4: Packet Delivery Ratio over 10% Attack Scenarios.

Figure 3 and 4 shows that 10 and 20 percent attacks Packet Delivery Ratio (PDR). PDR is slightly different than goodput, here we consider the control packets as well as data packets and no attack scenario PDR is not hundred percent due to channel collisions, mobility and congestion. Eventually the attacks severity in increasing order based on the above result is like this: Grayhole attacks, Rushing attacks, blackhole attacks, location discloser attacks, wormhole attacks.

In wireless mesh network, data packets can be dropped or delayed due to congestion, collisions, link failures and bit errors, and not because of malicious behaviour of the node. So that, any node drop or delay the packet, other nodes in the network can't treated as an attacker in that instance, instead they reduce the reputation value of the suspected node. Before declaring any node as malicious node, this process will be repeated until the reputation value gets zero of the suspected node. While reducing the reputation, "how much reputation we need to reduce of a suspected node?". In this case, our results are very useful if any node suspected as grayhole, reduce the small reputation value due to less severity of grayhole attack. On the other hand , if any node suspected as wormhole attack, reduce the large reputation value due to more severity of wormhole attack.

5. Conclusions

In this paper, we have studied various network layer attacks such as blackhole, grayhole, rushing, wormhole, location discloser, jellyfish and byzantine attacks, which are performed by malicious nodes. Based on malicious node behaviour we have identified their interdependencies. Furthermore, we have implemented these attacks in AODV routing protocol to find the severity of the attacks. Based on our simulations, wormhole attacks is more severe than any other attacks, on the other hand grayhole attack is less severe than any other attacks. We explained that how these severity metrics can be used for developing better security mechanisms.

References

[1] I. F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey, Computer networks, Elsevier 47 (4) (2005) 445-487.
[2] J. Xie, X. Wang, A survey of mobility management in hybrid wireless mesh networks, Network, IEEE 22 (6) (2008) 34-40.
[3] Zhang.Y, Security in Wireless Mesh Networks, CRC, 2008.
[4] Hoang.L, Uyen.T, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks 1 (2) (2003) 32-46.
[5] Muhammad.S, Choong.S, Security issues in wireless mesh networks, in: IEEE/IPSJInternational Symposium on Applications and the Internet, 2009, pp. 717-722.
[6] Ping.Y, Yue.W, A survey on security in wireless mesh networks, IETE TECHINICALREVIEW 27 (1) (2010) 6-14.
[7] Ricardo.C, Luiz.C, Ieee 802.11s multihop mac:a tutorial, Communications Surveys and Tutorials, IEEE 13 (2010) 52-67.
[8] H. Redwan, K.-H. Kim, Survey of security requirements, attacks and network integration in wireless mesh networks, in: New Technologies, Mobility and Security, NTMS'08, IEEE, 2008, pp. 1-5.
[9] Sahil.S, Anil.G, Current state of art research issues and challenges in wireless mesh networks, in: IEEE Second International conference on computer Engineering and Applications, 2006, pp. 1-17.
[10] Tamilselvan.L, Sankaranarayanan.V,Prevention of blackhole attack in manet, in: Wireless Broadband and Ultra Wideband Communications, International Conference on,Vol. 0, 2007, p. 21.
[11] Sharma, Parveen Kumar, and Rajiv Mahajan. "A security architecture for attacks detection and authentication in wireless mesh networks." Cluster Computing 20.3 (2017): 2323-2332.
[12] Xie, Ling Fu, and Et al. "A survey of inter-flow network coding in wireless mesh networks with unicast traffic." Computer Networks 91 (2015): 738-751.
[13] Reddy, K. Ganesh, V. Purushothama Raju, and P. Santhi Thilagam. "An effective analysis on intrusion detection systems in wireless mesh networks." Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on. IEEE, 2017.
[14] Alheeti, Khattab M. Ali, Anna Gruebler, and Klaus D. McDonald-Maier. "On the detection of grey whole and rushing attacks in self-driving vehicular networks." Computer Science and Electronic Engineering Conference (CEEC), 2015 7th. IEEE, 2015.
[15] Rathee, Geetanjali, and Hemraj Saini. "On Reduced Computational Cost, Efficient and Secure Routing (ESR) for Wireless Mesh Network." Procedia Computer Science 58 (2015): 333-341.
[16] Karri, Ganesh Reddy, and P. Santhi Thilagam. "Reputation-based cross-layer intrusion detection system for wormhole attacks in wireless mesh networks." Security and Communication Networks 7.12 (2014): 2442-2462.
[17] Reddy, K. Ganesh, and P. Santhi Thilagam. "Taxonomy of network layer attacks in wireless mesh network." Advances in Computer Science, Engineering & Applications. Springer, Berlin, Heidelberg, 2012. 927-935.
[18] Reddy, K. Ganesh, and P. Santhi Thilagam. "MAC layer security issues in wireless mesh networks." AIP Conference Proceedings. Vol. 1715. No. 1. AIP Publishing, 2016.
[19] Reddy, K. Ganesh, P. Santhi Thilagam, and Bommena Nageswara Rao. "Cross-layer IDS for rushing attack in wireless mesh networks." Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology. ACM, 2012.