International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Review on Security Issues in Mobile Adhoc Networks

Shetty Ashika Chandrashekar[1], Shetty Tanvi Shridhar[2], Vanyashree Mardi[3], Sanjana Shetty[4], Shreesha Bhat[5]

[1,2,4,5]*Student, Department of Information Science & Engineering, Alva's Institute of Engineering & Technology, Moodbidri, India*

[3]*Assistant Professor, Department of Information Science & Engineering, Alva's Institute of Engineering & Technology, Moodbidri, India*

***Abstract*: Mobile adhoc networks have gained tremendous importance due to their wide applications and necessity. Due to their to vast applications security in mobile adhoc networks have become an issue of great concern. There are various types of attacks to ruin a network out of which major are blackhole and wormhole attacks. Main causes of these attacks are unavailability of resources and alterations in the network topologies. Various algorithms and mechanisms have been proposed for detection and prevention of these attacks in the mobile adhoc network.**

***Keywords*: Mobile Adhoc Network, Blackhole Attack, Wormhole Attack;**

1. Introduction

Attackers are capable of disrupting the networks communication due to its open nature. A blackhole attack is the one in which a malicious node falsely claims that it has the shortest distance to the destination and thereby attracts the packets in network. In case of lack of security nodes of the network trust the malicious node and this ultimately results in loss of packets. A wormhole attack is the one in which the maliciousness is contained by a group of co–operating nodes connected via high speed channels preventing packet forwarding. A wormhole tunnel is formed which has a high transmitting rate and bandwidth due to which the nodes assume them to be the actual neighbors. Wormhole attacks are of three types namely open attacks, half open attacks and closed attacks. An open attack is one where all nodes of network know the node belonging to end of wormhole tunnel. In half open case only the network is aware of the malicious node taking the packet into the tunnel not the other nodes. In the closed type source and destination assume that they are away from each other by only one hop. Packet contents are modified so that actual nodes among wormhole nodes do not know the original hop. 3PAT algorithm is used to detect black holes, additional features of which also allow detection of wormhole attacks. The proposed algorithm works on an existing mechanism 3PAT [13] that detect the presence of black holes in the network. It has been extended to wormhole attacks by introducing some additional features. The algorithm also makes use of the fact that the wormhole nodes are not actually neighbors but act as if they are. There is no point in deploying malicious node as a cluster in the network. The attacker will have his slaves widespread in the network which is how he can actually attack the full network. So, the assumption that the wormhole attack nodes are distant but act as neighbors is strong in most of the cases.

2. Related work

A certificate based security mechanism that can detect wormholes in a network is being described by various authors. The certificate chaining is done by requesting the security parameters like neighbourhood, hop count, delivery rate and the certificate is issued only on satisfactory reports. In [3], the writer gave a detailed summary of the wormhole attack types, detection features and so on. She studied the various types of attacks with their requirements. The scholars [4] in their work compared the existing mechanisms for wormhole detection. The authors in [5] surveyed the Delphi approach proposed by Chiu that works on the basis of the fact that transmission of a packet within the tunnel does not involve more time than when the packets are sent in any other route by rescheduling. The author corresponding to [6] introduced a Trust based mechanism where the trust is brought by involving the nearest cluster head.

3. Proposed work

First apply the 3PAT [14] with every communication with the network. If there is any malicious behavior in the route, the 3PAT does well to find the Blackhole node. The Blackhole node may be the starting point of the wormhole tunnel. It may be the node that shall take your packet into the irrecoverable tunnel of the wormholes. At this node alone, we apply the transmission radius based algorithm to detect whether there is a chance for the detected Blackhole node to be a wormhole. The transmission radius based algorithm is slightly modified to make it fit into our problem. Whenever a black hole node is found by the 3PAT, the forwarding table of the node is checked. The checking is performed to find whether a group of nodes

were alone responsible for receiving the packets that were sent by the suspect node. If the cardinality of the group is very less, there are increased chances of finding the wormhole tunnel in association with our suspect. Those nodes which frequently receive packets from the suspect are subjected to the transmission radius based algorithm. The wormhole tunnel shall be detected by the transmission radius based algorithm, if any.

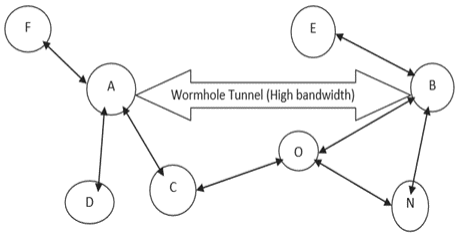

Fig. 1. A sample wormhole tunnel in a network.

The network in Fig. 1 shows eight nodes A, B, C, D, E, F, N, and O forming a WSN. There is a high bandwidth channel between A and B but it is not known to other nodes that it is a wormhole tunnel. A and B are not neighbors to each other but this channel gives the deception to the other nodes that they are neighbors to each other in the selected route is itself unlikely due to the precautionary measures taken in the algorithm. During the process of sending back every node in the path gets a unique until which the node is supposed to wait for the packet. The value is calculated based on the hop number and When a node does not receive a packet within the time factor limit, it generates the error message making us check for malicious behavior. All nodes after that reporting node start reporting the error in definitive time intervals. The part of the route that is behind the node that generated the first error is to be checked. The chance of a false misbehavior report is also nullified by looking at the routing table before taking any action. Thus, the 3PAT algorithm efficiently finds out black hole nodes, if present in the network.

Algorithm 3PAT:

1. Source sends RREQ to neighboring nodes.
2. Loop for each neighboring node (DEST not reached)
3. Increment the hop count
4. Transmit the RREQ with min. hop count.
5. End Loop.
6. If (DEST reached)
7. Select the RREQ with min. hop after authentication.
8. Make other RREQs Null or Invalid.
9. Calculate the time factor for D B. SYSTEM DESIGN.
10. Send the RREP along the route by calculating time factors for each node.
11. Else.
12. Repeat the process from Step-1
13. End If.
14. Send any data via the selected route.
15. If (any node doesn't receive packet in time)
16. Generate error report from the node.
17. Authenticate the report.
18. Return the node
19. Else
20. Return NULL
21. End if

The proposed solution is compared with a) using 3PAT only for wormhole detection and b) using transmission radius based algorithm for wormhole detection.

A. Using 3PAT only: 3PAT algorithm finds the presence of a Blackhole node with the time depending upon the position of the node in the path. Nearer the Blackhole node with respect to the source, lesser will be the time for the generation of the error report. Thus, for one complete loop of and messages it would require a time equivalent to the round trip time (RTT).

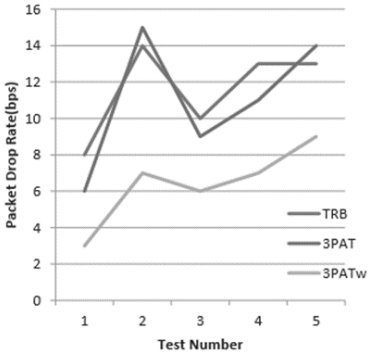

Fig. 2. Graph of no. of tunnels vs. Time taken for detection

The graph shown in Fig. 2 [15] describes the comparison of the proposed solution with the other approaches with varying number of wormhole tunnels. It is very clear that the detection of tunnel always takes lesser time for 3PATw than for 3PAT or TRB. Another point to note is that as the number of worm hole tunnels increase, the time taken also increases. This is due to the time taken for such transmissions to occur which will describe these nodes. If a single transmission can uncover all malicious nodes in the network, then only one transmission is needed to detect the tunnel.

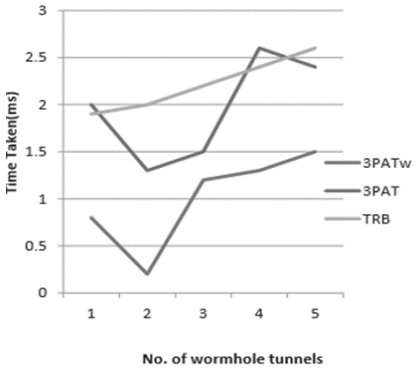

Fig. 3. Graph showing packet drop rate of all methods

The graph in Fig. 3, [15] shows the differentiation of the three methods with respect to the rate at which each method suffers from packet loss before detecting the maliciousness. It is clear that both 3PAT and TRB have had ups and downs in various test cases depending upon factors like position of wormhole tunnel in the network, the number of nodes in the tunnel, the configuration of the network, the link transmission speed of individual links, etc. But their counterpart namely the 3PATw is less sensitive to these factors and also suffers a comparatively lesser packet drop rate.

4. Conclusion

In our previous work, we proposed the 3PAT algorithm that was efficient towards single Blackhole node detection. But, it needed to be iterated over a number of times for a collaborative attack. Now, the proposed algorithm 3PATw overcomes the demerit of the existing method with respect to wormholes by taking features from TRB. We observed that the proposed scheme performs well than the traditional schemes in terms of packet delivery ratio and detection rate.

References

[1] E.A.Mary Anita, V.Vasudevan, A.Ashwini,"A CertificateBased Scheme to Defend Against Wormhole Attacks in Multicast Routing Protocols for MANETs", ICCCCT-10.
[2] Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET," International Journal of Computer Information Systems and Industrial Management Applications, Volume 3 (2011) pp. 271-279.
[3] Priya Maidamwar and Nekita Chavhan, "A survey on security issues to detect wormhole attack in wireless sensor network", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.
[4] Moutushi Singh, Rupayan Das, "A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network", International Journal of Scientific & Engineering Research Volume 3, Issue 10, October-2012.
[5] Jyoti Thalor, Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.
[6] Divya Goyal, Amrita Parashar, "Trust Computation Using DS in Sector Based Area to Detect or Preventing Wormhole in MAMET".
[7] Huaiyu Wen, Guangchun Luo., "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", Journal of Information & Computational Science 10:14 (2013) 4461–4476 September 20, 2013.
[8] Neeraj Arya, Upendra Singh, Sushma singh, "Detecting and Avoiding of Wormhole Attack and Collaborative Black hole attack on MANET using Trusted AODV Routing Algorithm", IEEE International Conference on Computer, Communication and Control (IC4-2015).
[9] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation (CSDI 2015).
[10] P.S.Hiremath, Anuradha T, Prakash Pattan, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs".
[11] Arun Kumar K A, "Wormhole-Black Hole Attack Detection and Avoidance in Manet with Random PTT using FPGA", 2016 International Conference on Communication Systems and Networks (ComNet), pp. 21-23 July 2016.
[12] Gu-Hsin Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network", EUASIP Journal on wireless communications and networking, 2016.
[13] R. Thanuja, A. Umamakeswari, Sri Ram. E, S. Dilip Kumar, "Three Phased Approach Towards Detection of Black holes in wireless sensor networks using time factor (3PAT)", Journal of Advanced Research in Dynamical and Control Systems, 2017.
[14] A linear time approach to detect mobile wormhole tunnels in mobile adhoc network using 3PAT and transmission radius (3PATw).
[15] Implementation of Blackhole Attack under Aodv Routing Protocol.
[16] Gilles Guette and Bertrand Ducourthial, ³On the Sybil attack detection in VANET´, IEEE, 2007.
[17] Pradip M. Jawandhiya, Mangesh M. Ghonge, M.S. Ali and J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks," International Journal of Engineering Science and Technology´, 2010.
[18] David B. Johnson, David A. Maltz and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891.
[19] Virendra Singh Kushwah, "Implementation of New Routing Protocol for Node Security in a Mobile Ad Hoc Network," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 9, December 2010.
[20] Preeti Nagrath and Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey," IEEE, 2011.
[21] 21.Abhijit Das, Soumya Sankar Basu and Atal Chaudhuri, ³A Novel Security Scheme for Wireless Adhoc Network´, IEEE, 2011.
[22] Farzad Sabahi, ³The Security of Vehicular Adhoc Networks," Third International Conference on Computational Intelligence, Communication Systems and Networks," IEEE, 2011.
[23] M. Ghonge, S. U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 2, Feb. 2012.
[24] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocols Stack A Review," IJEAT, 2012.
[25] Yi Zhang, Zhiyi Fang, Hongyu Sun, Lin Chen, "SARA: A Self-Adaptive Routing Algorithm in Wireless Sensor Network," 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, IEEE 2012.
[26] Mona N. Alslaim, Haifaa A. Alaqel, Soba S. Zaghloul, "A Comparative Study of MANET Routing Protocols," The Third International Conference on e-technologies and Networks for Development (ICeND2014), IEEE 2014.
[27] Parminder Kaur, Monika Sachdeva, Gagandeep, "Comparative Performance Analysis of MANET Routing Protocols," International Journal of Advances in Cloud Computing and Computer, 2016.