materialstoday: PROCEEDINGS

Volume 29, Part 2, 2020, Pages 348-351

Study on malicious node detection

Madhavi Dhingra [a], SC. Jain [a], Rakesh Singh Jadon [b]

https://doi.org/10.1016/j.matpr.2020.07.288 | Get rights and content

Abstract

Ad-hoc networks are a very popular form of wireless communication for mobile hosts where each node is free to move in the network. Networks are self-configurable and self-ruling systems consisting of routers and hosts, which can support movability and organise themselves randomly. More than that, other features such as frequent changes of the topology, nodes limits like energy, storage

Available online at www.sciencedirect.com

ScienceDirect

Materials Today: Proceedings 29 (2020) 348–351

materialstoday: PROCEEDINGS

www.materialstoday.com/proceedings

NSES 2018

Study on malicious node detection

Madhavi Dhingra[a*], S C Jain[a], Rakesh Singh Jadon[b]

[b]*Amity School of Engineering and Technology, Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP)-4740053*
[b]*MITS Gwalior*

Abstract

Ad-hoc networks are a very popular form of wireless communication for mobile hosts where each node is free to move in the network. Networks are self-configurable and self-ruling systems consisting of routers and hosts, which can support movability and organise themselves randomly. More than that, other features such as frequent changes of the topology, nodes limits like energy, storage device, CPU and communication channel limits like radio frequency, reliability add extra challenges. Mobile networks aimed to propose solutions to some basic problems, such as routing, successfully dealing with the new challenges caused by networks and nodes features without taking the security issues into account. Because of this, all these solutions are able to be hurt by threats. Any node under attack in network shows an weird and unexpected behavior called the evil and cruel behavior. This paper is a survey on different malicious node detection techniques in mobile networks.

Selection and Peer-review under responsibility of National Conference on Smart Materials: Energy and Environment for Smart Cities (NSES-2018).

Keywords: wireless communication, networks and nodes

1. Introduction

Mobile adhoc netowrk is the collection of wireless mobile nodes that communicate without any defined network infrastructure. This network follows temporary dynamic topology. A node can directly communicate with other nodes that are within the range. The nodes that are outside the range, are communicated with the help of intermediate nodes. Each node of Manet act as a router that forwards the packets to destination with the help of routing table. Thus, routing table is very important in the working procedure.

Security in Manet is very challenging as these networks follow the dynamic topology and work without any central base station. Traditional security procedures like firewalls, encryption techniques don't work here because of its features. Thus an improved, efficient Intrusion detection and prevention system is needed so as to secure the underlying system.

The MANETS are distributed and cooperative in nature. Different nodes share the resources for performing the functions in the network. Here, maintenance of resources is also a major issue. A single node can draw benefits from other network nodes while the same node can withdraw support in transmission of packets n the network. Such nodes are called selfish or misbehaving nodes as they show selfish attitude toward their peers [1,2].

* Corresponding author. Tel.:+91-9229125600.
E-mail address: mdhingra@gwa.amity.edu

Selection and Peer-review under responsibility of National Conference on Smart Materials: Energy and Environment for Smart Cities (NSES-2018).

Selfish or malicious nodes can send packets purposely to disturb the network traffic, and can disseminate false information about their connections in the network.Thus, misbehaving or malicious nodes is another important issue to be considered.

2. Related Work

Maintaining Security is the most important problem for researchers in Mobile Ad-hoc networks[3,4]. Due to the presence of dynamic topology and absence of central base station, the risk of vulnerability is high.Many schemes were proposed by the researchers for detection and prevention from malicious nodes which works on certain concepts like cryptography process, secure routing protocol, use of intrusion detection system and many more. The main focus of these detection schemes is to lower the rate of false alarm which happens when an honest node is identified as malicious node and vice versa.

2.1 Reputation Based Technique

The technique proposed by Josang [5,6] uses the concept of central authority network that is used for maintaining the reputation values of each node. Each node is associated with positive as well as negative feedback. Whenever a node wants to send packet, it send a request to central authority node for knowing the reputation value of other node. After certain interval, the reputation values get changed. But the main limitation of this method is in distributed network, where a single authority cannot maintain the reputation values of all other nodes. Further, prediction of reputation values in advance is also not possible.

This technique suffers from following drawbacks:

- The technique is based on functioning of central authority thus is not suitable for distributed network.
- The method of reputation computation is not a good approach for updation of reputation value
- The prediction of in advance reputation values is not possible.
- Relationships between the nodes cannot be drawn pictorially.

2.2 Punishment Based Technique

Punishment based technique is another variant of reputation based system. The process of detection and elimination of malicious nodes in the network is done in four sequential steps. Initial step involves the identification procedure for malicious nodes. The next step is about intimation of the presence of malicious node to all other nodes of the network. The third step is about assignment of reputation values to all the existing nodes. The final step is determination of the most efficient routing to transit the packets to the final destination without involving the malicious node [7]. This technique has a major drawback that routing table needs to get changed each time the reputation values got updated.

2.3 Incentive and Eigen Trust Technique

This technique uses the concept of charging for transmission of packets and compensating for forwarding the packets [7,8]. To reduce the charge of transmitting the packets, the node will take the packets from other nodes so as to forward it to another destination node. For such incentive purposes, virtual currency is used called as nuggets. Two kinds of nuggets are used - packet purse and packet trade model. In packet purse model, nuggets are added by the sender in the packets and the node that transmit the packets will receive the nuggets.In packet market model, every node will purchase the packet from its previous node by using some nuggets and sell it to the next node for some nuggets. With the same concept, Eigen Trust [9] is another technique based on the reputation, in which node ask all other nodes about the behaviour of all the nodes. Detection is identified based on the reputation of the nodes.

2.4 COOPMAC with ARQ

This technique[10] is based on Automatic Repeat Request protocol that works on the MAC layer of wireless mobile ad-hoc networks. Uniformly Most Powerful (UMP) and the Sequential Probability Ratio Test (SPRT) are used in the process. Let us assume that node P want to transmit the packet to node Q with the help of node R. The node P send the RTS packet in the network which contain the information about the link P-R and R-Q. Node Q send CTS packet to node P and node R send HTS packet to node R. On receiving both packets, node R will start the transmission. After recieving data from the nodes, the acknowledgement is sent to node P by ACK packet[11].
In this method, a node can behave either as the destination node or as cooperating node that will be used during process of packet transmission. The distributed Misbehaviour detection technique is used to detect the malicious nodes by checking the control packets.
In centralised detection approach, the special nodes decode the control packets and if any abnormal event is identified, then the same information is transferred to all the other nodes.
In CoopMacWith ARQ, the node transmit the data in the frame repeatedly until it gets the acknowledgement of the same frame. The destination node doest not store the old data packets and thus it is assumed for selfish nodes also. The UMP need more number of observations to identify malicious node while SPRT needs less number of observations.
The limitations of this approach are as follows:
• Traffic overhead increases in the network due to the transmission of control packets.
• High rate of delay in expected detection.
• An extra coop table need to be maintained to store the information regarding helping nodes.

2.5 Consensus Based Algorithms

Consensus based methods[12] are used for detection and elimination of malicious nodes from the network. It also detects the false positives. It calculates the probability of false alarm using the maximum cardinality technique. Stefano Tomasin [13] has proposed a consensus based algorithm to detect the malicious nodes and false alarm activity. A fusion centre is developed to merge all the local opinions into a single global one and while making of global opinions, false alarm of malicious nodes are considered. In some cases, a node can exist such that it is malicious with some nodes but works normally with all rest nodes. Such cases are handled by computing the values of em and n and sending it to the fusion centre. The centre will identify its validity and perform action with respect to the malicious nodes.
Inspite of the efficiency of the approach, there are still some weaknesses which include -
• the group of malicious nodes activities are not considered.
• High rate of delay in expected detection.
• Identification of malicious nodes using optimal method of clique search become more complex.

3. Conclusion

This paper has reviewed about several techniques to identify and remove the malicious nodes in the MANET. The malicious nodes effect the network negatively in terms of network performance, throughput, packet delivery count. Such nodes have a major impact on the routing protocol attacks. Due to this, the data transmission does not occur accurately between the source and the destination.
All the techniques helps in locating the malicious nodes and respond accordingly to provide efficient and robust transmission of packets between the nodes of the network.
From all the techniques, it is identified that an efficient system must have policies for identification of misbehaving, malicious nodes and elimination of such nodes. The policies should not impose additional overhead in terms of battery usage, additional computation, transmission complexity and storage system. It should be able to handle single as well as collection of malicious nodes that may try to violate the system.

References

[1] L. Buttyan and J.-P. Hubaux, “Security and Cooperation in Wireless Networks ,”http://secowinet.epfl.ch/, 2006.
[2] L.M. Feeney and M. Nilsson, “Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment ,” Proc. IEEE INFOCOM, 2001.
[3] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks ,” IEEE Network Magazine, vol. 13, no. 6, Nov./Dec. 1999.
[4] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks ,” Proc. Seventh Int’l Workshop Security Protocols, 1999.
[5] F. K. Hussain, E. Chang, and O. K. Hussain, “State of the art review of the existing Bayesian-network based approaches to trust and reputation computation,” in Proc. 2nd Int. Conf. on Internet Monitoring and Protection, July 2007.
[6] Audun Jøsang and Roslan Ismail, “The Beta Reputation System”, Proceedings of the 15th Bled Conference on Electronic Commerce, Bled, Slovenia, 17-19 June 2002.unpublished.
[7] Gopal R, Parthasarathy V, Mani A. Techniques to identify and eliminate malicious nodes in cooperative wireless networks. 2013 International Conference on Computer Communication and Informatics (ICCCI -2013); 2013 Jan 09-11; Coimbatore, India.
[8] Abrams Z, McGrew R and Plotkin S. A non-Manipulable Trust System Based on Eigen Trust. 2005, Jul; 5(4):21–30.
[9]S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the confidant protocol: cooperation of nodes–fairness in distributed ad hoc networks,” in Proc. 3rd ACM Int. Symp. on Mobile Ad hoc Netw. And Computing, 2002, pp. 226–236.
[10] S. Dehnie and S. Tomasin, “Detection of selfish nodes in networks using CoopMAC protocol with ARQ," IEEE Trans. Wireless Commun., vol. 9, no. 7, pp. 2328–2337, July 2010.
[11] Dehnie, Wayne and Tomasin. Detection of selfish nodes in networks using CoopMAC protocol with ARQ. Wireless Communications IEEE Transactions. 2010 Jun; 9:2328–37.
[12] Yu FR, Huang M, Tang H. Biologically Inspired Consensus-Based Spectrum Sensing in Mobile Ad Hoc Networks with Cognitive Radios. p. 26–30.
[13] Stefano Tomasin, “Consensus-Based Detection of Malicious Nodes in Cooperative Wireless Networks,” IEEE