Gyancity Journal of Electronics and Computer Science
Vol.3, No.2, pp. 25-28, September 2018
ISSN:2446-2918 DOI: 10.21058/gjecs.2018.32004

A Survey on Selfish Node Detection in Mobile Ad Hoc Network

Souvik Misra
Student of Computer Application Department(MCA)
Kalyani Government Engineering College West
Bengal,India

Abstract-- ***Mobile Ad-hoc Networks are self-configuring, infrastructure-less network for connecting the mobile devices. Security for this network is a big issue because of its frequently changing topology and dynamic nature. Some of it's nodes behave selfishly while preserving their own energy, thus the quality of the network goes down. In this paper we discussed about different kind of selfish node detection techniques in mobile ad-hoc network.***

Keywords-- ***Mobile Ad-Hoc Network, Selfish nodes, Security.***

1. Introduction

Mobile ad-hoc networks (MANET) are rapidly deployable, self-organized, self-configured and self-controlled infrastructure less networks. MANETs are decentralized in nature. Number of nodes changes very frequently as well as the links changes from one to another device. Every node is a router as well as end host. While transferring packets from source to destination packets moved through the intermediate nodes. Nodes in MANET takes part in the routing depending on their resources, hence as all the nodes are mobile in nature (e.g. laptops), they are battery driven. Thus battery life is considered as the resource. While transferring packets from source to destination sometimes the intermediate nodes drop the packets and the routing breaks down, this kind of nodes are known as selfish nodes. Selfish nodes drop the packets instead of forwarding them to the neighbor node to save their resources.

2. Attacks

Nodes present in the MANET refuse to participate in forwarding the packets are known as selfish node. Selfish nodes may simply refuse to forward without causing any damage to the network. Some of the nodes may agree to deliver packet and receives the packet, but instead of forwarding them they drop them. It causes damage to the network, these kind of attacks are known as passive attacks.

The other kind of attack is active attack. In this case the manipulative node enters into the network with high resources and start to send high amount of data in the network(flooding), this causes draining the energy of honest nodes. This kind of attack causes damage to the network. Nodes are prone to several attacks like black hole, worm hole attack.

In case of Black hole attack the malicious node declares that it has the shortest path for routing. A large amount of data comes to it and it has the authority whether to forward the data packets or to drop them.

In case of Worm hole attack two nodes which are causing black hole attack sum up together and attacks a large portion of the network.

3. Techniques of detection

Techniques used to find out the misbehaving nodes are discussed below:

Watchdog

In this technique the forwarding of packet between two nodes is being closely watched throughout the route. Thus when is dropping a packet it is identified and the route is avoided containing the misbehaving node.The major disadvantage of watchdog mechanism is: it is prone to error. The mechanism is not able to detect the packet collision, leads to false detection (both negative and positive). A minor dropping or nodes with limited resources (which are not able to transmit due to lack of battery life) are detected as misbehaving nodes. Another disadvantage is that the information about the misbehaving node is not spread within the network, thus only the node which has detected it gets benefited and other nodes remains unconscious about it. The selfish node is not punish instead of it the route is just avoided which affects the network in a broader way.

Random Feedback

In this scheme the sender attaches an encrypted note with the packet which is only decrypt able by the receiver node. Thus receiver can acknowledge each node by decrypting the note which is unknown to the intermediate nodes. Thus if a packet loss occurs it can be detected easily. But encrypting and decrypting every packet is quite expensive.

Pathrater

Each node identifies other nodes present in the network and maintains a degree of it. 'Path metric' for each node is calculated combined with the past experience with node's rating. Path having the highest path metric is chosen between all the reachable paths.

Credit Based System

In this system instead of punishing the misbehaving nodes, nodes which are performing honestly are being rewarded. To accomplish the target some kind of electronic payment methods are used to give rewards. This scheme is implemented by using two models: 1)The packet Purse model(PPM) and2) The packet Trade model(PTM).

Reputation Scheme

In this scheme nodes are being rated according to their behavior. A black list is maintained. Nodes with suspicious activity and poor rating are black listed. In this scheme black listed nodes remains within the network. The major disadvantage of this method is the non erroneous nodes also could be blacklisted due to false accusation.

CONFIDANT

Cooperatives Of Nodes-Fairness In Dynamic Ad-hoc Network (CONFIDANT) method detects and isolates the misbehaving nodes. In watchdog and pathrater the misbehaving nodes are avoided, they are not punished for their noncooperating behavior. Hence in CONFIDANT this issue is resolved, each node looks closely to the neighbor nodes. When information is found about misbehaving node it is spread to all the remaining nodes present in the network. The cooperative nature is evaluated with the Trust. How the nodes response in forwarding the packet is evaluated with Reputation. CONFIDANT consist of four components: 1)Monitoring 2)Reputation system 3)Trust Manager 4) Path Manager.

a) Monitoring : Nodes takes a close look to the neighbor nodes like the 'neighbor watch'. Transmission between the next nodes is observed by overhearing or observing the behavior according the route protocol. Thus the misbehaving nodes are detected.
b) Reputation System: A reputation table is maintained on the basis of the nodes. It is updated frequently by observing the past behaviors.
c) Trust manager: An ALARAM process is maintained. Each node has a trust manager which generates an ALARAM message on finding malicious node. When a node experiences, observes a malicious activity it generates an ALARAM message to the friends (who receives the messages). This message should be checked before reacting to it, because it can be generated from the outside of the friend list also.
d) Path Manager: As the name states the path manager decides which path to chose , how to react to a request. It decides the routing path on the basis of reputation of the nodes present on the path. It also takes an action receiving a request from the malicious node. When such kind of request occurs it alters the path or simply avoid that path.

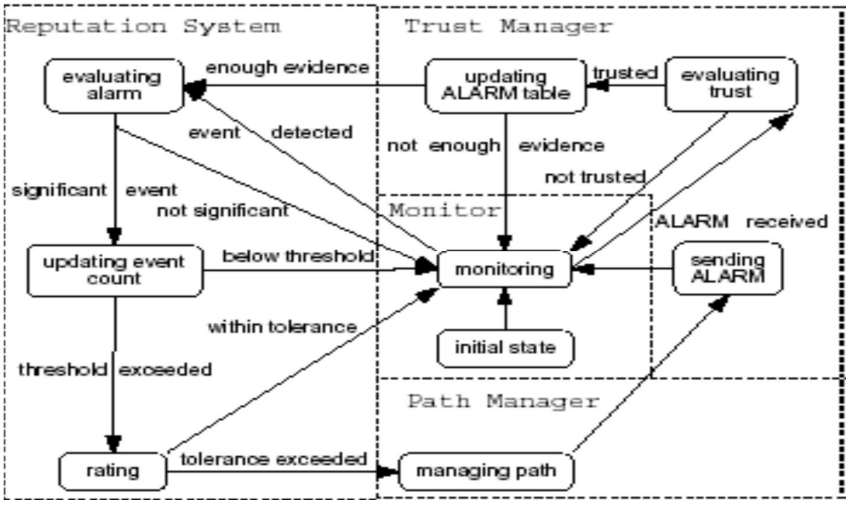

Fig. 1. CONFIDENT architecture

CORE

Collaborative Reputation mechanism (CORE) is quite similar with CONFIDANT mechanism. The key difference is in CONFIDANT both positive and negative reports are allowed where a CORE only allows the positive ones. We have seen that sometimes nodes doesn't misbehave intentionally, they ran out of resources and wrongly interpreted as malicious nodes. In CORE architecture a reputation table is maintained. In the reputation table the past activities of the nodes are recorded as their rating. When a node denies from forwarding packet CORE decreases its rating. The rating starts from zero and gradually increases with every forwarding. If a node has a very low rating, it is declared as malicious node. Each node's behavior is decided depending on factors like observation, positive rating by others, and depending on specific task.

To prevent the network from malicious node CORE doesn't allow to give negative rating it only can give a positive rating. So malicious nodes trying to decrease the rating of other node is impossible.

In CORE the false accusation is prevented. CORE is not able to prevent increase of rating of malicious node through colluding nodes.

OCEAN

OCEAN (Observation-based Cooperation Enforcement in Ad hoc networks) proposed by Bansal and Baker[1], is a stand alone architecture as it observes by itself and don't depend upon others ratings to check the false accusation.It divides the misbehaving nodes into two types First ones are the nodes which enters into the path but refuse to forward packet and leads to misleading. Second ones don't show up on rout discovery and known as selfish nodes.

A checksum mechanism is used here. If node fails to forward packet after receiving it within a given time period then the nodes rating is updated as negative or positive. A threshold limit is maintained. If a nodes goes below the faulty threshold limit it is detected as a malicious node. No request from that node is taken.

A rewarding system is also available, every time when a node forwards a packet its cheapcount goes up. A node with a cheapcount below the threshold limits are considered as selfish nodes. Any kind of request from it is rejected.

Routeguard

Routeguard technique divides the nodes into four categories. This categorization is based on present and past behavior of the node while forwarding a packet. The watchdog and pathrater technique is used to categorize the nodes. The categories are:

1. Fresh
2. Member
3. Unstable
4. Malicious

Depending on their category nodes are allowed or not allowed to take part in the route.

Ex Watchdog

It is an extended version of watchdog. As we have seen watchdog overhears the transmission between each node and try to identify the malicious node. But if the malicious node itself hears the transmission then the problem occurs. This problem is resolved in this mechanism, it reports about the malicious node which is trying to participate in the network.

4. Conclusion

In this survey paper we have discussed about various selfish node detection techniques in MANET. As the usage of MANET is rapidly growing security is becoming very important aspect. In our future work we will discuss about different attacks that can take place MANET and how to prevent them.

ACKNOWLEDGEMENTS

Dr. Anuradha Banerjee, teacher of Department of Computer Applications, Kalyani Govt. Engg. College, West Bengal, India has helped me throughout this survey.

REFERENCES

[1] S.Bansal and M.Baker, "Observation-based cooperation enforcement in ad hoc networks" Stanford University,Tech. Rep., 2003.
[2] Parker J, Undercoffer J, Pinkston J, Joshi A. (2004). "On intrusion Detection and Response for Mobil Ad Hoc Networks", in Proceeding IEEE International Conference on Performance Computer and Communications, Workshop on Information Assurance, pp 747-52.
[3] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in (CMS'02), September 2002.
[4] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks)," in Proc. IEEE/ACM Workshop on (MobiHoc'02), June 2002, pp. 226–336.
[5] Hasswa A, Zulkernine M, Hassanein H. (2005). "Routeguard: an intrusion detection and response system for mobile ad hoc networks", in Proceeding IEEE (WiMob'2005).
[6] Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1
[7] S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc.
[8] 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), August 2000, pp. 255–265.
[9] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," in WCNC 2004, 2004.

[10] Farzaneh Pakzad and Marjan Kuchaki Rafsanjani "Intrusion Detection Techniques for Detecting Misbehaving Nodes",in Computer and Information Science Vol. 4,-1; January 2011
[11] Caballero E J. (2006). "Vulnerabilities of intrusion detection systems in mobile ad hoc networks- the routing system", Seminar on Network security, Helsinki University of Technology.
[12] Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network, in Proceeding IEEE (ICC'07), pp 1154-9.