International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Survey on Watchdog Systems and Classifier Based Scheme to Detect Selfish Nodes in MANET

K. Yasotha[1], R. Gunasundari[2]

[1]Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education

[2]Research Supervisor, Department of Information Technology, Karpagam Academy of Higher Education

Abstract: ***Mobile Ad-hoc Networks (MANETs) is self configured and decentralized wireless network without any prior infrastructure. Every node in it acts as a router as well as end-system and hence each node in MANET is allowed to move freely which makes routing difficult. Combine effort of nodes in Mobile Ad hoc Network makes it more powerful. But supporting a MANET is a cost-intensive activity for a mobile node. Finding routes and forwarding packets consumes bandwidth and energy. One such routing misbehavior is that some nodes may be act as selfish by participating in route discovery and maintenance process, but deny forwarding the packet. Such nodes routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. MANETs lack a centralized monitoring and management point, making it a challenging task to detect such misbehaving nodes effectively.***

Keywords: Watchdog, selfish node, MANET

1. Introduction

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANET does not depend on pre-existing infrastructure or base stations. A mobile node can become a failed node for many reasons, such as moving out of the transmission ranges of its neighbors', exhausting battery power, malfunctioning in software or hardware, or even leaving the network.

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer or any other device capable of sending and/or receiving data generated by other nodes on the network. Mobile ad-hoc networks (MANETs) are composed of mobile nodes connected by wireless links without using any pre-existent infrastructure**.**

A selfish node is one that tries to utilize the network resources for its own profit without sharing its own resources to others. Selfish node will certainly avoid itself from the routing paths because it might delay the Route Request (RREQ) packet up to the maximum upper limit time. The selfish node can participate in routing messages but it does not forward the data packets. .

A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing time to live (TTL) value to smallest possible value. A selfish node did not forward the data packets and hence other nodes may not be able to detect its presence when they need it. The major reason for such behavior is low residual battery power, faulty software and hardware. Selfish node does not intend to involve itself in the network damaging activities such as Ip spoofing and so on. Hence we conclude that a selfish node is not a malicious. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. Watchdog helps to detect the selfish node.

Working principle of watchdog is to maintain a buffer of recently sent packets and comparing each overheard packet. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold, it determines that the node is misbehaving and spread the message to the source that it is a misbehaving node. The formulae for watchdog "Number of incoming message is equal to Number of outgoing message".

1.1Selfish Node Behaviors

Selfish nodes are inclined to get the greatest protects from the networks and at the same time these nodes trying to conserve their own resources like bandwidth, [1] battery life or hardware. A selfish node only communicates to other nodes if its data packet is required to send to some other node and refuses to cooperate other nodes whenever it some data packets or routing packets are received by it that it has no interest in. Hence data packets are either refused to retransmit or are dropped for being received by a selfish node. The selfish nodes behaviors in AODV routing protocols can be as follows:

1) Nodes which do not send Hello packet: The principle target of this sort of selfish node is hiding itself and to abstain from being included in the others transmission way.
2) Nodes which do not forward RREP messages: Because of this kind of selfish behavior whole network will be paralyzed. In AODV, the source node will get a RREP message from the destination node through some intermediate nodes to establish a complete transmission path, but here the communication path will not be established because this kind of selfish nodes will not forward the RREP message. Hence the source node will broadcast Route Request (RREQ) message continuously.
3) Nodes which do not forward Data messages: The misbehavior of this type of selfish node impacts the performance of MANET by dropping all the data

messages that are received by these nodes. Instead of relaying these data messages these will be dropped.

4) Nodes forwarding RREQ messages with delay: When this kind of selfish node gets a Route Request(RREQ) message it forwards this RREQ message after some lag near the upper bound of time out for not to participate in a route.
5) Nodes which do not forward RREQ messages : In MANET, if this type of selfish nodes receives some RREQ messages, then instead of forwarding these RREQ messages, these messages are dropped and thus these kind of selfish nodes skips being the route member for other nodes. Thus avoiding forwarding these messages for others as a result more nodes are required for building a transmission path.
6) Selfish Behaviors Depending on the Nodes Energy: This type of selfish nodes acts normally if its energy level lies between full energy level and some threshold k1. They act like do not forward data messages selfish node if its energy level lies between k1 and some k2 and if its energy level is below k2 then they behave like do not forward RREQ message selfish node.

1.1. Applications of MANET

With the increase in the portable devices and in addition advance in wireless communication, ad hoc networking is picking up imperativeness as a result of its growing number of far reaching applications. Ad hoc networking could be connected anyplace at any time without any framework and its adaptable networks. Ad hoc networking permits the nodes to keep up connections to the network and in addition effectively adds and expels nodes in and out from the network.

Emergency services
- For replacing fixed infrastructure in case of ecological disasters
- Fire fighting and policing
- Emergency rescue operation
- Support in hospital for nurses and doctors

Sensor Networks
- Body area networks (BAN)
- For tracking movements of animals, detection of biological/chemical environment conditions.

Enterprise and home networking
- Office/home wireless networking.
- Meeting rooms, conference hall, personal area networks (PAN) personal networks (PN).
- Construction site networks.

Tactical networks
- Military objects moving at high speed such as tanks, warships and airplanes.
- Battle fields which are automated.

Commercial, civilian and education environments
- Networks of visitors at airports.
- Virtual classrooms, universities and campus settings.
- Ad hoc communications during meetings or lectures.

2. Detection of Selfish Nodes

A selfish node detection technique for MANET must also deal with the following issues arising from constraints imposed by their specific environments and applications [10]:

- **Network partitioning:** Due to presence of selfish node, network partitioning occurs more often in MANET. Network partitioning is a severe problem in MANET when the server that contains the required data is isolated in a separate partition, thus reducing data accessibility to a large extent.
- **Data Availability:** The loss of some links and nodes considered as critical can split up the network into several disjoint partitions in the presence of selfish nodes. Mobile nodes in one of
- the partitions cannot access the data held by the mobile nodes in the other partition. This situation considerably reduces data availability.
- **Network life time:** In MANET, network performance becomes highly dependent on collaboration of all member nodes. A selfish node will typically not cooperate in the transmission of packets for saving its resources, it seriously affecting network life time.
- **Throughput:** Percentage of packets received by the destination to the number of packets sent by the source is affected by available of selfish nodes in
- MANET.
- **Hop count**: A hop is the segment of the route between the source and destination nodes. Each node along the data routing path comprises a hop. If number of Selfish nodes increases in MANET, Number of intermediate hops from source to destination increased. It could be decreased the performance of the Network.
- **Packet dropping Ratio:** Number of packets dropped by the routers due to nodes act as a selfish node for saving its resources.
- **Packet Delivery Ratio:** It is the fraction of the number of data packets delivered to the destination node from the source node. It is affected by selfish
- node in MANET.
- **End-to-End delay:** End-to-end delay is the time consumed by a data packet to be transferred across the MANET from a source node to the destination node. It is increased by selfish nodes in MANET.
- **Probability of Reachability:** Fraction of possible reachable routes to the all possible routes between all different sources to all different destinations.

1.2. Detection techniques

Techniques used to detect selfish nodes can be classified into the following three categories:

Reputation Based Scheme:

This scheme works in a collaborative manner. Reputation simply means to opinion about a thing. Here nodes communicate with each other in order to give feedback about particular nodes cooperative behaviour. Every node gives feedback in terms of a reputation value. In this way every node collects high reputation value to build trust and confidence about good behaviour and cooperation in network. Low reputation value is considered to be indication

of selfish behaviour while high reputation value indicated cooperative behaviour of nodes. The reputation value of a selfish node is clear indication to the other nodes about its cooperation in the network. The network will detect the selfish nodes then the message about this will get propagated to the entire network and the selfish node will be eliminated from the network [2].

Credit Based Scheme:
In this scheme [3], incentive is given to cooperating nodes for the transmission function in network. Main idea here is "serve & earn". This incentive based scheme uses the concept of virtual credit or electronic currency or similar payment schemes. The incentives are given for packet forwarding in order to motivate the non-cooperative node to participate. This scheme needs a setup virtual payment system. It uses two models as-
(i) The Packet Purse Model:
(ii) The Packet Trade Model:

Acknowledgement Based Scheme:
The acknowledgement based schemes ensures the forwarding of a packet by a node using an acknowledgement. In this scheme a node sends an ack packet to source once it is being forwarded. If a source node does not get this ack packet this means misbehaviour of node is observed [4].

ACK Scheme
K. Balakrishnan et. al. [4] have proposed a scheme called 2ACK scheme which is a network layer scheme to detect the selfish nodes. This scheme uses an acknowledgement packet called 2ACK packet for detection. In this scheme the next hop node in the route will send back the 2 hop acknowledgment packet ie 2ACK. This acknowledgment packet is used to indicate that the data packet has been received successfully. The first router from the sender will not serve as the sender of 2ACK.

Watchdog:
Marti et. al. [3] have proposed the watchdog mechanism which is implemented on every node. It monitors nearby nodes in order to identify the misbehaving nodes. When a node forwards a packet to the watchdog, it checks whether the next node in the path will forward this packet or not. If watchdog observes that if the node does not forwarding the packet then it is considered as selfish node. The watchdog will avoid such selfish nodes from the routing path and selects alternative path. In the following Fig 3.1. Node S is a source and node D is a destination. Node S forward the packets to node Watchdog present in node S overhear the neighbor node A whether it forwards the packets to neighbor node B. Here node A forwards the packets to node B. Similarly, watchdog present in node A overhears whether node B forward the packets to node D. The problem with watchdog is partial dropping; false misbehavior, limited transmission power, receiver collisions and ambiguous collisions might not be detected.

Figure 2.1: Watchdog

Path rater:
Marti et. al. [3] has proposed this mechanism where a path metric is calculated for each routing path. This is achieved by setting up a mechanism called as path rater with every node. Each node runs this mechanism and gives rating after every successful transmission of packet. After calculating the path metric for every path to the particular destination, the path with highest metric will be chosen as the most reliable path.

CONFIDANT
Buchegger et. al. [5] have proposed a technique which is somewhat similar to watchdog and pathrater and it is known as CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad Hoc Networks). The CONFIDANT protocol contains four important components i.e. Monitoring System, Reputation System, Trust Manager and Path Manager.

CORE:
Michiardi et. al [6] have proposed CORE (Collaborative Reputation Mechanism) system to improve the coordination among nodes. It uses two basic components which are 1) Reputation table and 2) Watchdog mechanism. It enforces the cooperation among the nodes by using reputation report mechanism. Each node performs some computation to calculate the reputation value for all neighbour nodes. The reputation report contains values ranges from positive to negative. This mechanism allows to pass only positive reputation reports.

OCEAN:
Bansal et. al. [7] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks). It also uses the monitoring and reputation mechanism. The OCEAN mechanism is basically having following five components 1) Neighbors Watch 2) Route Ranker 3) Rank-Based Routing 4) Malicious Traffic Rejection and 5) Second Chance Mechanism.

SORI:
Q. He et.al. [8] have proposed secure and Objective Reputation-based Incentive (SORI) scheme. This method encourages the packet forwarding. It consists of three components and they are (1) Neighbour monitor, (2) Reputation propagation and (3) Punishment.

Sprite:
Zhong et. al. [9] have proposed a scheme called Sprite. It uses a Credit Clearance Service (CCS). It is used to define the credit and charge of each node. To calculate the charges and credits it uses Game theory methods. Each node will get a receipt of message that it has received or forwarded. Each node keeps the receipt of the message and it will forward the receipt to the CCS. The credit of a node is totally depending on the forwarding behaviour of a node. The forwarding is considered as successful only if the next node on the path reports a valid receipt to the CCS. If the node forwards the message then credit will be raised otherwise credit decreases.

3. Classifier based scheme to Detect selfish nodes

A mobile ad hoc network (MANET) is an infrastructure-less network. In mobile ad hoc network, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes in order to save its own resources. This behavior of selfish nodes could then degrade the overall data accessibility which results into performance degradation of overall network.

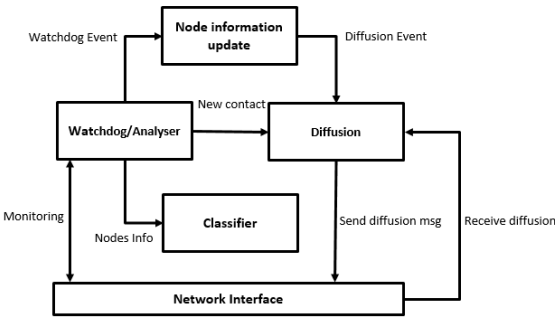

Figure 3.1: Framework

Process:
Following is the actual process of proposed system.

Input: Path (Source to Destination)

Processing:
a) Path formation and selfish node is generation.
b) Communication overhearing by watchdog.
c) Behavior message diffusion to neighboring nodes
d) Packet data analysis submission to Classifier.
e) Classification Process

Output: Selfish Node Detection

States in System:
In proposed system nodes have four states [Fig.3.1].
a) Initial state: Initially node does not have any information about any selfish node
b) Selfish contact (Positive) : It is a state when a node detects a selfish node using its watchdog and historical record
c) Collaborative contact: It is a state when contacts between pairs of nodes occurs to transmit there detection
d) Information.
e) Partial Selfish contact (Positive): It is a state when a node detects a partial selfish node using its watchdog and historical record

4. Conclusion

In this paper, several issues concerning developing Reputation based selfish node detection in mobile ad-hoc networks have been discussed. Selfish or misbehaving nodes degrade overall system performance and cause a serious threat to multihop routing in MANETs.

Reputation based models play an important role in detecting and isolating selfish nodes. Many approaches are available in the literature. But no approach provides a finite solution to the selfish nodes problem. The detection and isolation mechanism isolates the selfish nodes so that they don't receive any services from the network, thus penalizing the selfish nodes. But what happens if many nodes become selfish Network communication itself will become impossible. Thus we cannot eliminate all the selfish nodes from the network. A new mechanism to be designed to reduce the effect of selfishness and to stimulate the nodes to cooperate in the network services.

References

[1] Wu, Lien-Wen, and Rui-Feng Yu. "A threshold-based method for selfish nodes detection in MANET." Computer Symposium (ICS), 2010 International. IEEE, 2010.
[2] Y. Yoo, S. Ahn, and D. Agrawal, "A credit payment scheme for packet forwarding fairness in mobile ad hoc networks", In Proceedings of IEEEICC, volume 5, pages 3005 – 3009 Vol. 5, may 2005.
[3] 3 . S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), August 2000, pp. 255–265.
[4] K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005
[5] S. Buchegger et al., "Self-policing mobile ad hoc networks by reputation systems". Communications
[6] Magazine, IEEE, 43(7):101 – 107, July 2005.
[7] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in (CMS'02), September 2002.
[8] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks" Stanford University, Tech. Rep., 2003.
[9] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation based incentive scheme for ad-hoc networks," in WCNC 2004, 2004.
[10] S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile AdHoc Networks", Technical Report, Yale University, July 2002, pp. 1987-1997.
[11] Wu, Lien-Wen, and Rui-Feng Yu, "A threshold-based method for selfish nodes detection in MANET." Computer Symposium (ICS), 2010 International IEEE, 2010.