A Survey of Techniques Used To Detect Selfish Nodes in MANET

Karthik M[1] Jyothish K John[2]
[1]M. Tech [2]Associate Professor
[1, 2]Department of Computer Science and Engineering
[1, 2] Federal Institute Of Science And Technology, Angamaly, Kerala, India

Abstract— An mobile Ad Hoc network is a collection of mobile nodes. They do not have any existing infrastructure and they do not have any centralized administrator. So the MANET is self-creating, self-organizing and self-administrative wireless network. In MANET each node acts as router. In practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and bandwidth for retransmitting the data of other nodes. They will preserve the resources for their own use. In this paper we have provide the comparative study of different type of methods to increase the selfish node detection and the network throughput

I. INTRODUCTION

A mobile Ad Hoc network is a collection of mobile nodes. They do not have any existing infrastructure and they does not have any centralized administrator. So the MANET is self-creating, self-organizing and self-administrative wireless network. In MANET each node act as router. These nodes in the network are responsible discovering the path to the particular node and forward the data to that node. Since the nodes in the network have the capability of moving so the infrastructure of network will change rapidly. Each node in the MANET will forward the data to other node but some nodes will not forward the data packet to other nodes they are called the selfish nodes. The selfish node in the network will cause the different problems in network.

Each node in the network has its own resources such as bandwidth, energy, local CPU time and transmission power etc. The selfish nodes will reduce the cooperation among the nodes in the network. While the selfish nodes trying to preserve their resources such as battery life or bandwidth, they will get the benefits from the networks. The selfish node will forward its own data packet but it will refuse to forward the data packet of the other nodes. The selfish node can perform the actions such as do not participate in the routing process, turn off the power when there is no communication with other nodes, do not send hello or no reply messages, does not unicast or broadcast the Route Error packet, selectively drop the data packets etc. The selfish nodes in the network will reduce the packet delivery ratio by dropping the data packets. The selfish node detection is important to increase the performance of the ad hoc networks in practical applications.

II. SELFISH NODE DETECTION METHODS

The selfish node detection methods can be categorize into (1) reputation based schemes (2) credit based schemes and (3) acknowledgement based scheme

A. Reputation Based Schemes

The reputation value in the case of a selfish node is the indication to the other nodes about the perception about the cooperation of a node. The network will collectively detect the selfish and suspicious nodes then the declaration will propagated to the entire network and the selfish node will be eliminated from the network. If the reputation value of a node is low then the node is considered to be selfish by other node. If the reputation value is high then the node is cooperative

B. Credit Based Schemes

In order to perform networking functions faithfully by nodes the credit based schemes will provide incentives to nodes. This kind of strategy stimulates nodes increase the cooperation among the nodes by utilizing the the concept of virtual credit or electronic currency or similar payment schemes. There are two model for implementing the credit based schemes 1) The Packet Purse Model 2) The Packet Trace Model [01]

C. Acknowledgement Based Schemes

The acknowledgement based schemes will uses the acknowledgement packet to ensure the packet is forwarded by the node. If the node does not receive the acknowledgement from a node, that means that node not forwarding the data packet. Based on the acknowledgement it detect the selfish nodes

III. DETECTION SCHEMES

A. Watchdog

In Kachirski O et. al. [02], the watchdog of the node will identify the misbehaving nodes by monitoring the nearby those nodes. When a node forwards a packet to the watchdog will verifies or check whether the next node in the path will forward the packet or not. After checking if watchdog finds that if the node does not forward the packet it considered as selfish or misbehaving. The watchdog will eliminate the selfish nodes from the path and the implementation is easy. The advantage of watchdog is it can identify misbehavior node in link layer and network layer. The disadvantages of watchdog are it can't detect the misbehavior nodes in case of limited transmission power, ambiguous collision, receiver collision, minor dropping etc.

B. Pathrater

In Kachirski O et. al. [02], in this mechanism each node running a pathrater, each node in the network maintain a rating for all other nodes in the network. The "path metric" for every path is calculated by each node. After calculating the path metric for every path to the particular location, the

path with highest metric will be chosen as the reliable path and it is decided by the pathrater. The advantage of pathrater is the throughput increases with the increase in node mobility. The disadvantage of pathrater is overhead in the transmission increases with increase the mobility

C. CONFIDANT

In Buchegger et al [03] proposed a technique similar to watchdog and pathrater, i.e. CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad Hoc Networks). This method will detect the misbehaviour node by monitoring the behaviour of neighbour nodes and they will pass this information to all other nodes, the misbehaviour node will not be punished. The CONFIDANT protocol contains four modules, Monitoring System, Reputation System, Trust Manager and Path Manager. Each of the modules has some specific task to perform. CONFIDANT protocol is an expansion of DSR protocol. The advantages of CONFIDANT protocol is the throughput increases, overhead of extra message is low and the disadvantage of CONFIDANT protocol is node authentication is not checked.

D. CORE

In Michiardi et. at [04] proposed CORE (Collaborative Reputation Mechanism) to detect the selfish nodes, the mechanism also improve the coordination among nodes. It increases the cooperation among the nodes by using reputation mechanism and collaborative monitoring. The reputation values ranges from positive to negative through null. Each node computes the reputation value for all neighbour nodes. The basic components used in the CORE mechanism are 1) reputation table and 2) watchdog mechanism. The advantages of CORE mechanism are it will prevent the DOS attacks, it is impossible for a node to maliciously decrease another node's reputation because there is no negative rating spread between nodes. The disadvantages are CORE suffers from spoofing attack, it cannot prevent colluding nodes from distribute negative reputation

E. OCEAN

In Bansal et al [05] proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks).OCEAN also uses the monitoring and reputation mechanism. The OCEAN layer reside on each node and have basically five components 1) Neighbour Watch 2) Route Ranker 3) Rank-Based Routing 4) Malicious Traffic Rejection and 5) Second Chance Mechanism. Each node has rating, after monitoring there is a negative or positive event is produced and uses this event to update rating of other nodes. The nodes are added to the faulty list if the rating is lower than the threshold. The advantages of OCEAN are it will distinguish the selfish and misleading nodes, network throughput increases. The disadvantage is it is failed to punish the misbehaving nodes severely.

F. 2ACK Scheme

In Manvia et. Al [06] proposed a scheme called 2ACK scheme, it is a network layer scheme to detect the misbehaviour nodes. This scheme uses a acknowledgement packet called 2ACK packet to detect the selfish nodes. where the next hop node in the route will send back the 2 hop acknowledgment packet ie 2ACK ,this to indicate that the data packet has been received successfully. The first router from the sender not serves as the sender of 2ACK. The advantages of the schemes are it checks the confidentiality of message, increase the packet delivery ratio y detection and scheme can be added to any source routing protocol. The disadvantages are it will cause the traffic congestion on the network.

G. SORI

In He et.al [07] proposed Secure and Objective Reputation-based Incentive (SORI) scheme. It detects the selfish nodes and encourages the packet forwarding. Reputation rate of a node is based on the packet forwarding ratio of nodes. SORI consist of three components they are neighbour monitor, reputation propagation and punishment. The packet forwarding behaviour is monitored by neighbour monitor and shares this information to other nodes by use of reputation propagation. Punishment will use the information of evaluation record of a node and the threshold to make decision about the packet dropping. The advantages of the schemes are SORI is computationally efficient as compared to other methods and it reduces the communication overhead. The disadvantages are SORI does not differentiate between misbehaviour and selfish nodes and SORI has poor performance in the case of cooperation node

H. LARS

In Hu et.al[08] proposed a scheme called Locally Aware Reputation System (LARS). This scheme finds the misbehaviour and encourages the cooperation among nodes. There are evaluator nodes they will evaluate the reputation value of the nodes. Each node will maintain the reputation value of its one hop neighbours and they will update their reputation value based on the neighbour behaviour. There is an threshold for reputation value of anode if the reputation value falls below the threshold then it is considered as misbehaving by the evaluator node. Evaluator node uses WARNING message to notify the neighbours about the Misbehaviour. The advantages of the schemes are the misbehaviour node is not completely excluded from the network, after a time out it can re-join to network such as it must increase its reputation by increase the cooperation. The disadvantages are, the power consumption of evaluator node is high and message overhead is high.

Sprite in Zhong et. al [09] proposed a scheme called sprite. In which a CCS (Credit Clearance Service) is introduced. It will determine the credit and charge of each node. Game theory methods are used to calculate the charges and credits. Each node will keep the receipt of the message its received and it will forward the receipt to the CCS. The credit of a node depends of the forwarding behaviour of a node. If the next node on the path reports a valid receipt to the CCG then only the forwarding is considered as successful. A node will get more credit if it forwards the message otherwise its credit decreases. The advantages of the scheme are it can be applied to unicasting protocol and can extend to multicasting also. The disadvantages are, the collusion attack is possible and it is difficult for CCS to calculate the payment

I. Secure Incentive Protocol

In Yanchao et.al [10] proposed SIP (Secure Incentive Protocol). SIP uses the credit as the incentive to stimulate packet forwarding. Here each mobile node has a security module and they deal with the security related functions. The credits of the node increases and decreases depend on the forwarding behaviour of the node. Whenever a node is initiating or forwarding a packet first node will pass it to sip module for processing. SIP is session based and consists of four phases, 1) Session Initiation 2) Session Key Establishment 3) Packet Forwarding And 4) Rewarding Phase. The advantages of the scheme are SIP is routing independent; it is session based rather than packet based and unauthorized access is not allowed. The disadvantage of SIP is it implemented on hardware module so each node to possess a hardware module.

J. AAS Scheme

In Gunasekaran et.al [11] proposed Authenticated Acknowledgement Based Scheme (AAS) for preventing the selfishness in mobile Ad Hoc networks. This scheme is similar to 2ACK scheme. Which assign a fixed route of three nodes (two hops) in the opposite direction of data traffic route. A methodology must be performed by sending and receiving nodes if they wish to communicate with each other. There is a password for each transmitting packet and it will contain the data. A tag for data is formed by applying the hash function to the password. So the sending packet will contain hash value, data and tag. The advantages of the scheme are which ensure the integrity, confidentiality and authentication to the data transmitted, it increases the packet delivery ratio and throughput by increasing the selfish node detection. The disadvantages are it increases the overhead of transmission and end to end delay, AAS does not consider the weak links Detection of Selfish Nodes Using Credit Risk In Jae-Ho Choi et.al [13] proposed the credit risk to find out the selfish nodes. The credit risk can be described by the following equation

$$credit\ risk = \frac{expected\ risk}{expected\ value}$$

Each node will calculate the credit risk for the other nodes to which it is connected. Based on the score each node will detect the selfish nodes. In each relocation period, the nodes will calculate the credit risk. Each node has the predefined threshold value for the credit risk. Each node will calculate the credit risk and if the calculated credit risk greater than threshold then the node is a selfish node. Expected value and expected risk are calculated based on the node specific features.

IV. COMPARISION

Approach	Routing Overhead	Throughput	False Positive	Scalability	Limitations
TWOACK Scheme	High	Increases	High	Yes	Traffic Congestion
S-TWOACK Scheme	High	Increases	Low	Yes	Low packet delivery
Watchdog And Pathrater	Low	Increases	High	Yes	Ambiguous Collision,
Reputation Based Scheme	Low	Increases	Low	Yes	Node Authentication Is Not Checked
Intrusion Detection System	Low	Increases	Low	Yes	Ids Is Not Energy Efficient
AAS scheme	High	Increases	High	Yes	It Increases The End To End Delay
Ccs (Credit Clearance Service)	Low	Increases	Low	Yes	Collusion Attack Is Possible
Cooperative Intrusion detection system	Low	Increases	Low	Yes	Changed AODV implementation
Secure Incentive Protocol	High	Increases	High	Yes	Every Node To Possess A Hardware Module
SORI (Secure And Objective Reputation Based Incentive)	Low	Increases	Low	Yes	Poor Performance
LARS	Low	Increases	Low	Yes	Not Energy Efficient
OCEAN	Low	Increases	High	Yes	Failed To Punish The Misbehaving Nodes

V. PROPOSED METHOD

A. Combined collaborative watchdog and credit risk to detect the selfish node

Here we are proposing a combined scheme for the detection of selfish nodes. In the credit risk method each node will find out the selfish node individually so the detection time of the method is high. On order to reduce the detection time we are using the collaborative watchdog [14]. Collaborative watch dog is based on contact dissemination ie if one node has a previously detected selfish node then using its watchdog it can send this information about the selfish node to other node when a contact occurs. The detection of the contact can be easily found out using watchdog. The watchdog will overhear the packet of the neighbouring nodes. The information about the selfish nodes is called the positives. When a node receives the packet from the other nodes it assumes it is a new contact, then the node will send all its all known positives to the newly contacted node. Here the node detection is performed by credit risk method and the detected information is passed to the other nodes by collaborative watch dog so the detection time will reduces.

The node has two states NONINFO and POSOITIVE, in the NONINFO state the node has no information about the selfish nodes and POSITIVE state the node has information about the selfish node

VI. CONCLUSION

As the use of Mobile Ad hoc Networks (MANETs) has increased, the MANETs security has become more important. The selfish nodes will reduce the cooperation among the nodes in the network .Selfish nodes are a real problem for ad hoc networks since they affect the network throughput. This paper discussed several approaches for dealing with selfish nodes. Many approaches are available in the literature. But no approach provides a solid solution to the selfish nodes problem. The Credit based approach provides incentives to the well behaving nodes and just by passes the selfish nodes in selecting a route to the destination. But selfish node still enjoys services without cooperating with others. The detection and isolation mechanism isolates the selfish nodes so that they don't receive any services from the network.

REFERENCES

[1]. Farzaneh Pakzad and Marjan Kuchaki Rafsanjani "Intrusion Detection Techniques for Detecting Misbehaving Nodes", in Computer and Information Science Vol. 4,-1; January 2011.

[2]. Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1.

[3]. Buchegger S, Le Boudec J. (2002). "Performance analysis of the CONFIDANT protocol (Cooperation of nodes fairness in dynamic ad-hoc network)", in Proceeding 3rd ACM (MobiHoc'02), pp 226–336.

[4]. Michiardi P, Molva R. (2002). "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in International Conference on (CMS'02).

[5]. Bansal S, Baker M. (2003). "Observation-based cooperation enforcement in ad hoc networks", in Technical Paper on Network and Internet Architecture (cs.NI / 0307012). [6]. Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi "USING A TWO-TIMER SCHEME TO DETECTSELFISH NODES IN MOBILE AD-HOC NETWORKS" in Proceeding of the sixth IASTED July 2-4, 2007

[7]. He, Q., Wu, D., Khosla, P., 2004. "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks" in WCNC'04 IEEE Wireless Communications and Networking Conference.

[8]. Hu, J., Burmester, M., 2006. "LARS: a locally aware reputation system for mobile ad-hoc networks", in 44th annual ACM Southeast Regional Conference

[9]. S. Zhong, J. Chen, and Y. Yang, "Sprite: A Simple, Cheat-Proof, Credit- Based System for Mobile Ad-Hoc Networks", Technical Report, Yale University, July 2002

[10]. Yanchao Zhang , Wenjing Lou , Wei Liu, Yuguang Fang," A secure incentive protocol for mobile ad hoc networks" in Journal of Wireless Networks , Volume 13 Issue 5, pp. 663-678 , October 2007

[11]. M. Gunasekaran1, P. Sampath, B. Gopalakrishnan" AAS: Authenticated Acknowledgement Based Scheme For Preventing Selfish Nodes In Mobile Ad Hoc Networks "in International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009

[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

[13]. Jae-Ho Choi, Kyu-Sun Shim "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network",in ieee transactions on mobile computing, vol. 11, no. 2, february 2012

[14]. Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate." Collaborative Watchdog to Improve the Detection Speed of Black Holes in MANETs "

