Journal of Theoretical and Applied Information Technology
20th February 2014. Vol. 60 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY ON REPUTATION BASED SELFISH NODE DETECTION TECHNIQUES IN MOBILE AD HOC NETWORK

[1]S.SENTHILKUMAR, [2]J.WILLIAM

[1]Assistant Professor, Department of CSE, University College of Engineering, Pattukottai,Tamilnadu,India

[2]Professor, Department of IT, M.A.M College of Engineering, Tiruchirappalli, Tamilnadu, India

E-mail: [1]senthilucepkt@gmail.com, [2]wills.susan@gmail.com

ABSTRACT

Mobile Ad hoc Network (MANET) is well known for its limited transmission range of wireless network interface. Hence, multiple hops (multi-hops) may be needed for exchanging the information from one node to another across the network without any base stations or routers. In MANETs, as there is no hierarchy among nodes, every node is responsible for forwarding packets to its neighbouring nodes. Due to severe resource constraints like memory, computing power, energy, bandwidth and time, some nodes may not participate in forwarding the packets for saving its resources. The presence of selfish behaviour among nodes may lead to network partitioning and makes a major negative impact in throughput and the network operation. To avoid such circumstances selfish node deduction is very important. Already many selfish node detection mechanisms have been developed and still exist. And this survey is to evaluate some of the reputation based selfish node detection mechanisms and to analyze its merits and demerits. This paper compares different methods based on QoS metrics as well as on node's behavioral analysis for reducing the effect of selfish nodes in mobile ad hoc networks.
Keywords: *MANET, Multi-Hops, Selfish Nodes, QoS.*

1. INTRODUCTION

A set of autonomous wireless mobile nodes constructing a temporary network without the aid of a centralized infrastructure called Mobile Ad hoc Networks [1, 24] (MANETs), which communicate through multiple hops (Multi-hops). In such type of networks, each mobile host performs two different roles of acting itself as an end system, as well as of a router by forwarding packets to its desired destination nodes. Hence the nature of MANETs makes cooperation among the nodes essential for the system to be operational. In addition, the issues of wireless channels such as the limited data transmission range, low bandwidth, high error rate environment, and limited battery power, makes routing in MANETs complicated to deal with. Indeed, nodes try to preserve their resources, and particularly their batteries. Due to this fact, some nodes are not willing to forward packets to other nodes such type of nodes are called misbehaving nodes. The presence of these misbehaving nodes results in potential danger that threatens the quality of service, as well as one of the most important network security requirements, namely the availability. But these nodes have no intention of damaging the network.

The characteristics of misbehaving nodes as follows:

- ***Do not contribute in routing process*:** A selfish node is not forwarding the routing messages or it modifies the TTL (Time To Live) values of the Route Request and Reply packets.
- ***Do not reply or send hello messages***: A selfish node does not respond to hello messages, hence other mobile nodes unable to detect its occurrence when they require it.
- ***Deliberately delay the RREQ packet*:** A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.
- ***Dropping of data packet*:** A selfish node may participate in routing messages but may not forward data packets

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

So as to increase the existence of their devices, mobile nodes may fell forced to show a selfish behaviour. Selfish behaviour threatens the entire community because of Optimal paths may not be available and cooperative nodes may become overloaded and be forced to discard the community. Several selfish node detection techniques explored to minimize the network performance degradation, loss of sent packets, network partitioning. This survey mainly focuses on the features, the advantages and the disadvantages of each and every technique in detection of selfish nodes in MANETs. The importance of this study is to compare all the QoS metrics and nature of misbehaving nodes.

The remainder of this paper is organized as follows. Section 2 discusses the various issues concerning selfish node in MANETs. Based on the issues, Section 3 classifies the existing reputation based selfish node detection techniques for MANET. Section 4 review the Existing selfish node detection techniques using the established criteria. Section 5 presents a comparison of all the Reputation based selfish node detection techniques in this paper. Finally, Section 6 concludes the paper and identifies future research directions.

2. ISSUES CONCERNING SELFISH NODE IN MANET

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

- **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.

These issues could potentially lead to network partitioning and corresponding performance degradation. To minimize such

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

situations in MANETs, many studies have explored in Reputation based selfish node detection techniques.

3. REPUTATION BASED TECHNIQUES: OVERVIEW

In a reputation based technique, each node is responsible for monitoring the transmission of a packet to neighbour node, or obtaining the status of other nodes from a centralized node on the network. If a node successfully contributes in the transmission of data by forwarding data packets, the reputation of the node is increased, or if the node discards the packet by dropping it, the reputation is decreased. After the nodes reputation drops below a threshold set by the developer, the node is either punished or ignored. The following Figure 1 represents the classification of different reputation based techniques for selfish node detection in MANETs.

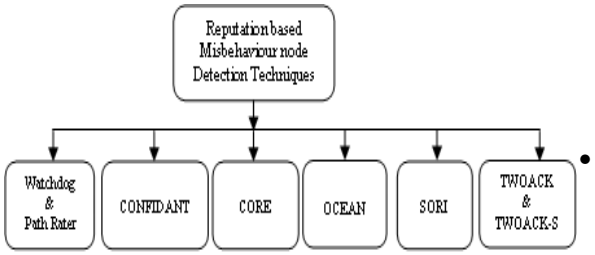

Figure 1: Classification Of Reputation Based Selfish Node Detection Approaches.

Watchdog technique has been proposed by Marti, Giuli, Lai and Baker [2]. Each node has a mechanism which overhears the medium to check whether the next-hop node faithfully forwards the packet or not. Each node maintains buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If it overhears forwarding, removes the packet from the buffer and determined that node as a normal node. If a packet has stayed in the table for longer than a certain period, the module increments a failure count for the node responsible for forwarding on the packet. If the count exceeds a certain threshold value, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

The Strength of this mechanism is to detect selfish node accurately and to maintain the throughput of the system at an adequate level even with a more number of misbehaving nodes and it can identify selfish node in link layer and network layer. This scheme has several bottlenecks.

- It can't detect the selfish nodes in case of limited transmission power, ambiguous collision, receiver collision, minor dropping etc.
- It is only suitable for source routing protocols such as DSR instead of any general routing protocols.
- This technique does not penalize the selfish nodes that not cooperate and really omits them of the load of forwarding for others. As a result, being selfish becomes a blessing to MNs themselves.
- The watchdog can work only when links are bidirectional. In practical, many unidirectional links may exist in MANETs due to the topology control.
- Each mobile node requires certain amount of memory space to store packets until proper forwarding by its neighbour is confirmed. These stored packets are used for a comparison with packets forwarded by its neighbouring MN to check and ensure if the neighbour transmits correct data. As a result, it consumes high volume of storage.

Marti, Giuli, Lai and Baker [2] proposed pathrater technique for selecting reliable path from source to destination. In this mechanism, each node in the network maintains a rating for all other mobile nodes. It computes "path metric" by averaging the rating of the nodes on the paths and the metric gives a comparison of the overall reliability of different paths.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. If any node gets very low rating, it should be considered as a selfish node and thus excludes them from routing.

It concentrates to select the reliable path but not deals with recovering the selfish node in MANET. The advantage of pathrater is the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

throughput increases with the increase in node mobility. The main drawbacks of this approach are that it does not punish selfish nodes and if the mobility of nodes increases overhead also increases.

Finally this mechanism does not measure for punishment against selfish nodes that do not cooperate with others, but rather relieves them of the load of forwarding for others.

3.2 CONFIDANT

The CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc NeTworks) protocol is effective technique for detecting misbehaving node proposed by Buchegger and Le Boudec [3].The objective of this approach is detecting and isolating misbehaving nodes. In this approach, Reputation and trust value is calculated based on the observation and experience about behaviour of other nodes. The following Figure 2 represents the components of The CONFIDANT mechanism such as a monitor, reputation system, trust manager and path manager.

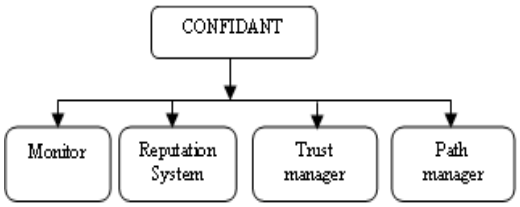

Figure 2 Components of CONFIDANT

- **Monitor**: It is responsible for observing and recording the selfish of neighbouring nodes.
- **Reputation system**: Each node maintains a list of local node ratings for each one of its neighbours, which could be exchanged with its unselfish neighbours.
- **Trust manager:** It is responsible for sending warning of misbehaving nodes.
- **Path manager:** It is responsible for punishing paths that contain misbehaving nodes, re-ranking paths according to the reputation of nodes in the path, and deciding what should be done when a misbehaving node requests a path or an unselfish request a path containing misbehaving nodes.

The advantages of this approach are no data forwarding service (punishment) is provided for low reputation nodes i.e. misbehaving nodes, it avoids possible bad routes and throughput increases even though mobility increases.

The drawbacks of CONFIDANT are

- Inconsistent problem occurs due to each node has different evaluations for same node to detect the selfish node.
- Eavesdropping is not addressed.
- Nodes in a black list are ignored.
- Need more battery power consumption for a node located in the centre of network in comparison to situated at the periphery of the network.
- Scalability is another problem due to key validation and certification in the trust manager.
- Friend making is not well established

3.3 CORE

In Michiardi and Molva [4] proposed CORE (Collaborative Reputation Mechanism) to detect and isolate selfish nodes. The mechanism also improves the coordination among nodes by using reputation mechanism and collaborative monitoring. CORE classifies three types of reputations, which are combined to form a common reputation value for a mobile node. Each metric is normalized so that a reputation ranges from –1 (bad) to +1 (good). 0 represents a neutral view, and this is used when there are not enough observations to make an accurate assessment of a node's reputation. First, Subjective reputation [-1, 1], is calculated based on past observations. Second, Indirect reputations (positive reports by others) are observed by node *X* from node *Z* about node *Y* only positive reputation values are used, to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

eliminate an attack where a selfish node transmits negative reputation information to cause a denial-of-service. Third, functional reputation that combines the subjective and indirect reputation which is gradually decreased to a null value if there is no interaction with the observed node. The advantages of CORE mechanism 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 limitations of CORE suffers from spoofing attack, it cannot prevent colluding nodes from distribute negative reputation, Limited transmission power and directional antennas have not been addressed.

3.4 OCEAN

In Bansal et al [05] proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the DSR protocol. OCEAN also uses the monitoring and reputation mechanism. The components of OCEAN on each node specified in figure 3.

In neighbor watch module, it monitors the behaviour of the neighbours of a node. Route Ranker module calculates and maintains ratings for each of the neighbouring nodes. Rank-based Routing module helps to omit routes containing nodes in the block list. Malicious Traffic Rejection discards all traffic from nodes it decides misleading. Finally, Second Chance Mechanism is provided to give another opportunity to operate as normal nodes that were previously considered misbehaving nodes.

The advantages of OCEAN are it will distinguish the selfish and misleading nodes, it maintains overall network throughput with existence of selfish nodes at network layer. It fails to punish the misbehaving nodes severely.

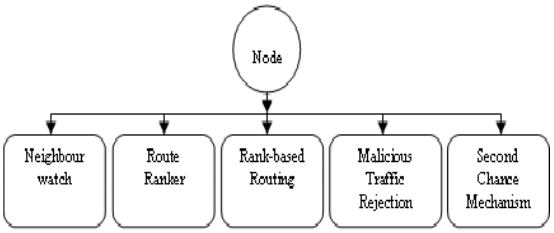

Figure 3 Components of OCEAN

3.5 SORI

He et.al [06] proposed Secure and Objective Reputation-based Incentive (SORI) approach for Encouragement of packet forwarding and discipline selfish behaviour using reputation based punishment mechanism. Reputation value of a node based on packet forwarding ratio of nodes. It has three modules for neighbour monitoring, reputation propagation and punishment.

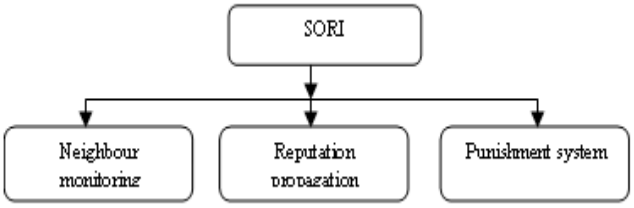

Figure 4 Components of SORI

Neighbour monitoring system is responsible for to collect information about packet forwarding behaviour of neighbours that is node N keeps count of number of packets sent by node N to the node X for forwarding, called RFN(X)(request for forwarding) , and number of packets actually forwarded by node X for node N, called HFN(X) . Reputation of a node is computed using these values. Trust value of a node is directly proportional to number of packets forwarded through the node (RFN(X)). Trust value is used to give high priority to the reputation value received from the node.

Reputation propagation system is responsible for communicating reputation of nodes among neighbours when there are significant changes in reputation of some node(s). One way hash chain is used for authentication of reputation information messages and data packets.

Punishment system is responsible for deciding the probability of dropping packets of a misbehaving node in proportion of its selfish.

The merits of the scheme are computationally efficient as compared to other methods and it reduces the communication overhead. It fails to differentiate between malicious and selfish nodes. It also has poor performance in the case of cooperation node.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.6 TWOACK

The existing techniques suffer from several bottlenecks such as ambiguous collisions, receiver collisions, unidirectional links, partial dropping and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link. To overcome this problem, Balakrishnan [07] has proposed a TWOACK scheme, which focuses on the problem of detecting misbehaving links instead of misbehaving nodes. TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehaviour by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is selfish node. So normal nodes became part of misbehaving link and therefore cannot be further used the network and it will cause the traffic congestion on the network.

3.7 S-TWOACK

The TWOACK scheme described above gives rise to two hops of TWOACK packets for every hop of data packet being forwarded. Considering that each TWOACK packet is a unique entity and has to contend for the medium just like any other packet, the TWOACK packets may contribute to the traffic congestion on the routing path. Therefore, Balakrishnan [07] further proposed the S-TWOACK (Selective-TWOACK) scheme, a derivative of the TWOACK scheme, to reduce this extra traffic due to TWOACK packets. In the S-TWOACK scheme, instead of sending back a TWOACK packet every time when a data packet is received, a node waits until a certain number of data packets (through the same triplet) arrive. The node then sends back one TWOACK packet acknowledging multiple data packets that have been received so far. So in this scheme, a significant reduction of routing overhead achieved.

4 COMPARISON

In this survey, we summarize eight approaches for selfish node detection which use different inputs and reputation evaluation function. We have seen that some proposals may cause higher communication overhead, while some do not use any special packets at all. In Watchdog and Pathrater approach, improve high system throughput even in existence of misbehaving nodes. In CONFIDANT, CORE and SORI approaches to enforce cooperation by punishing misbehaving nodes and motivating them to act correctly. The purpose of the OCEAN system is to completely isolate misbehaving nodes from the network. In TWOACK and S-TWOACK, Solve the problems of Ambiguous and receiver collusions and not affected by limited transmission power and overhearing range problem. We summarized features of the Surveyed Schemes in Table 1.

5 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] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[2] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug. 2000, pp.255-265

[3] S. Buchegger and J. –Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks," Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, CH,9-11 June 2002, pp.226-236.

[4] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *The 6th IFIP Conf. on Security Communications, and Multimedia*, Porotoz,Slovenia, 2002.

[5] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," *Research Report .NI/0307012*, Stanford University, 2003.

[6] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad- Hoc Networks," *Proc.IEEE Wireless Communications and Networking Conf.*, vol. 2, pp. 825-830, March 2004.

[7] K. Balakrishnan, J. Deng, and P.K.Varshney," TWOACK:Preventing selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC'05),Mar. 2005.

[8] X. J. Li, B.-C. Seet and P. H. J. Chong, "Multihop cellular networks:Technology and economics," *Computer Networks*, Elsevier, vol.52, No.9, pp. 1825- 1837, Jun. 2008.

[9] Y. Yoo and D. P. Agrawal, "Why does it pay to be selfish in a MANET," *IEEE Wireless Communications Magazine*, vol. 13, issue 6,pp. 87-97, Dec. 2006.

[10] Y. Liu and Y.R. Yang, "Reputation Propagation and Agreement in Mobile Ad-Hoc Networks," *Proceedings of IEEE Wireless Communications and Networking Conference WCNC*, vol. 3, pp. 1510 – 1515, Mar. 2003.

[11] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations",RFC 2501, Jan. 1999.

[12] Capkun S, Buttyan L, Hubaux JP,"Self-Organized public-key management for mobile ad hoc networks", IEEE Transaction on Mobile Computing; 2003:52-64.

[13] Yongwei Wang, Venkata C. Giruka, Mukesh Singhal, "A fair distributed solution for selfish node problem in mobile ad hoc networks", Proceedings of ADHOCNOW'04, 2004.

[14] S. Buchegger and J. Y. Le Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", In Proc. of P2PEcon,2004.

[15] A. A. Pirzada, C. McDonald and A. Datta, "Performance comparison of trust-based reactive routing protocols", IEEE Trans. on Mobile Computing, vol. 5, no. 6, 2006, pp.695-710.

[16] S Buchegger and J.-Y. Le Boudec,"Self-policing mobile ad hoc networks by reputation systems", c*ommunications Magazine,IEEE*, 43(7):101–107, Jul 2005.

[17] M. Conti, E. Gregori, and G. Maselli,"Cooperation issues in mobile ad hoc networks", In *ICDCSW '04: Proceedings of the 24th International Conference on Distributed computing Systems Workshops - W7: EC (ICDCSW'04)*, pages 803–808,Washington,DC, USA, 2004. IEEE Computer Society.

[18] A. Baadache, A. Belmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Journal of Network and Computer Applications 35 (2012) 1130–1139.

[19] S. Chengqi, Z. Qian, "OMH - Suppressing Selfish Behavior in Ad Hoc Networks with One More Hop", SpringerLink Mobile Networks and Applications, 14 (2009) 178-187

[20] Kejun Liu, Jing Deng, P.K. Varshney, K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, 6 (2007) 536 - 550

[21] F. Kargl, A. Klenk, S. Schlott, M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks", Lecture Notes in Computer Science: Security in Ad Hoc and Sensor Networks 3313 (2005) 152–165.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: A Comparison Of The Selfish Node Techniques

Features	Watch Dog & Pathrater	CONFIDANT	CORE	OCEAN	SORI	TWOACK	S-TWOACK
Design	Distributed	Distributed	Distributed	Standalone	Distributed	Distributed	Distributed
Underlying Protocol	DSR	DSR	DSR	DSR	AODV	DSR	DSR
Layer	Data link & Network	Network	Network	MAC & Network	Network	Network	Network
Observation	Passive	Passive	Passive	Passive	Passive	Active	Active
Detection	Single node	Single node	Single node	Single node	Single node	Single node	Single node
Punishment	No	Yes	Yes	Yes	Yes	Yes	Yes
Computational Overhead	Low	Low	Low	Low	Low	Low	Low
Communication Overhead	Low	Low	Low	Low	Low	High	High
Throughput	Higher than DSR	Higher than DSR	Higher than DSR	Higher than defenceless and global reputation schmes	increases	increases	increases
Energy Consumption	Low	High	High	Low	High	High	High
False Positive	High	Yes	Partially restricted	High	Low	High	Low
Robustness Against collusions	No	Yes	No	No	No	No	No
Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Second Chance Mechanism	No	No	No	Yes	No	No	No
Inspection Source to neighbour	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inspection Neighbour to others	No	No	No	No	No	Yes	Yes
Considered Attackers	Selfish nodes & Malicious node	Selfish nodes	Selfish nodes	Selfish nodes	Selfish nodes	Selfish nodes	Selfish nodes