# A Survey of Misbehavior Detection Scheme in DTN

M. Balaganesh
Associate professor, Dept of CSE Sembodai Rukmani varatharajan Engineering College,
Sembodai, Tamilnadu

P. Sathiya
PG Scholar, Dept of CSE
Sembodai Rukmani Varatharajan Engineering College,
Sembodai, Tamilnadu.

D. Balagowri
PG Scholar,Dept of CSE
Sembodai Rukmani Varatharajan Engineering College,
Sembodai, Tamilnadu

## ABSTRACT

The survey tries to review the various problems and their solution in Delay Tolerant Network (DTN) while routing the packets. In this paper, going to discuss and see the overview of various methods used in the DTN. They are simbet and bubble rap which are the DTN routing algorithm and is used for identify the bridge nodes using betweenness centrality and similarity metrics in the network. Then watchdog and pathrater used for detecting the misbehaving nodes in the DTN. Practical incentive protocol (Pi) is used for addressing the selfishness problem in DTN. Secure multilayer credit based incentive scheme (SMART) provide the incentives to the selfish node by using credits in the network.

## Keywords

DTN, practical incentive protocol, simbet, bubble rap, watchdog, pathrater, SMART.

## 1. INTRODUCTION

Delay tolerant networks (DTN) are a communication network designed to withstand disturbance and outages. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data and forwarding decisions are made by locally collected knowledge about the behavior of nodes [7]. Routing protocols are used such as SIMBET and BUBBLE RAP [3],[8]. Simbet used for detecting the nodes which are the part of same community and betweenness centrality. And for identify bridging nodes which could travels a message from one community to another community. Bubble Rap is similar to simbet protocol. It is also used for search the bridging nodes from source to destination community. Mitigating routing works by using neighborhood monitoring or destination acknowledgement to detect packet dropping.

The watchdog is used for detect and isolating misbehaving nodes. The main aim of the watchdog is to improve the performance of the network under the presence of malicious nodes. The pathrater combines the link reliability with knowledge of misbehaving nodes. Each and every node maintains a rating for other node for knowing about the network. The pi protocol is focus on the fairness issue in DTN. By using the practical incentive protocol the performance of the DTN can be improved in the terms of low average delay and high delivery ratio. SMART is used for stimulate bundle forwarding cooperation among DTN nodes. SMART scheme can be implemented in a distributed manner for thwart different attacks without relying on tamperproof hardware. In existing works considering only either of misbehavior detection or incentive scheme. iTrust is a probabilistic misbehavior detection scheme to achieve efficient trust establisment in DTNs. The proposed iTrust scheme is inspired from the inspection game , a game theory model in which an inspector verifies if another party, called inspectee, adheres to certain legal rules. TA, is launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then, TA could punish or compensate the node based on its behaviors. Therefore, an efficient and adaptive misbehavior detection and reputation management scheme is highly desirable in DTN. The performance of the misbehavior detection scheme improved by the reputation system. In reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability. A game theoretical analysis used for analyzing to demonstrate that TA could ensure the security of DTN routing at a reduce cost by choosing an appropriate investigation probability. The proposed evidence framework could not only detect various misbehaviors but also be compatible to various routing protocols. Correlating the user's reputation to the detection probability which is expected to further reduce the detection probability. By using the extensive simulation as well as detailed analysis for demonstrate the effectiveness and the efficiency of the iTrust. iTrust has two phases, including routing evidence generation phase and routing evidence auditing phase. In the evidence generation phase, the nodes will generate contact and data forwarding evidence for each contact or data forwarding. In the subsequent auditing phase, TA will distinguish the normal nodes from the misbehaving nodes. Two types of algorithm are Basic misbehavior detection algorithm and Proposed probabilistic misbehavior detection algorithm. The basic misbehavior detection algorithm itself incurs a low checking overhead. It is used to prevent malicious users from providing fake forwarding/contact evidences. The proposed probabilistic misbehavior detection algorithm is used as a inspection game and demonstrate by setting an appropriate detection probability. By using this algorithm, achieving a lower detection overhead and still stimulate the nodes to forward the packets for other nodes.

## 2. RELATED WORKS

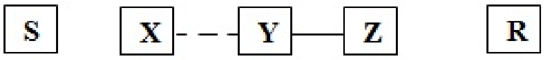
Delay tolerant network is a communication network designed to withstand long delays or outages. It is capable of storing packets in intermediate nodes until such time as an end-to-end route can be established. Some protocols used in DTN network are discussed below.

## 3. SIMBET AND BUBBLE RAP

Simbet and bubble rap [3], [8] are the two DTN routing algorithm. Simbet routing is a social based routing protocol which is proposed by Daly and Haahr. It is used to identify some bridge nodes in the network using betweenness centrality and similarity metrics. The algorithm defines the communication between the two nodes are represented by the simber routing. Considereig that two nodes name as node 'n' and node 'm'. If receiving a hello message , node 'n' verifies that node 'm' is a new neigbour node. In this situation , any data send for node 'm' are delivered and an encounter request is sent. Node ‘m’ sends the reply message with a list of nodes it has encountered. The list of contacts are used for update the betweenness valuse on node ‘n’ and the similarity value on ‘m’ and used for betweenness calculation and similarity calculation. Bubble rap is a social based forwarding algorithm. Bubble rap selects the high centrality nodes and community members of destination. The first part of the strategy for forwarding is to send the messages to the nodes which are most familiar than the current node. The second part of the strategy for forwarding is to identify the destination community members.

## 4. WATCHDOG

Watchdog is a scheme which is proposed by Marti et al [14]. The watchdog is used for detect and isolating misbehaving nodes. The main aim of the watchdog is to improve the performance of the network under the presence of malicious nodes. The watchdog method is used for detecting the misbehaving nodes. Watchdog method is implemented by maintaining a buffer. Buffer stores the packets which was recently sent and compare each and every overhead packets with the packets stored in buffer for watching in if there is a match or not. If the packets are match , the packet is removed from the buffer. The watchdog technique has weakness and advantages. The advantages is that it can detects the misbehaving node at the level of forwarding. The weakness of watchdog are that it might not detect the node which are misbehavior at the presence of collusion ,limited transmission power, ambiguous collisions, false misbehavior, partial dropping collusion.



The fig1 shows that when y forwards a packet from S towards R through Z, X can overhear Y’s transmission and can verify that Y has attempted to pass the packet to Z. The solid line represent the intended direction of the packet sent by Y to Z, while dashed line indicates that X is within transmission range of Y and can overhear the packet transfer.

## 5. PATHRATER

Each node in the network can run the pathrater [14]. For pick the route most likely to be reliable. The pathrater combines the link reliability with knowledge of misbehaving nodes. Each and every node maintains a rating for other node for knowing about the network. The rating assigns to the node according to the algorithm. The pathrater assigns node as “neutral” rating of 0.5, when a node in the network is known to the pathrater. A node in the network always rates 1.0 itself. By fixing the rates it ensuring that if all the other nodes are in neutral nodes at the time of calculating the path rate. The shortest length path choosen by the pathrater.

## 6. PRACTICAL INCENTIVE PROTOCOL

The practical incentive protocol called as Pi [12,10,2]. This protocol is used for address the selfishness problem in DTN. By using the practical incentive protocol the performance of the DTN can be improved in the terms of low average delay and high delivery ratio. The pi protocol is focus on the fairness issue in DTN. The pi attaches some incentive on the bundle when source node sends a bundle message which is fair to all participating DTN nodes. The practical incentive protocol consists of four parts. They are system initialization, bundle generation, bundle forwarding and charging and rewarding. The pi protocol provides the various security issues. They are fair incentive, free ride attack, layer adding attack and layer removing attack. The free riding attack is a notorious selfish attack in DTN. In layer removing attack, the previous layers on the forwarding path are removed by the selfish intermediate node. The layer adding attack could be launched, when system allows DTN node with multiple identities.

## 7. SMART

A secure multilayer credit-based incentive scheme called as SMART [6] [1] [9] [16]. SMART uses credits for provide incentives to selfish nodes in the network. It is used for stimulate bundle forwarding cooperation among DTN nodes. SMART scheme can be implemented in a distributed manner for thwart different attacks without relying on tamperproof hardware. SMART is proposed for DTNs afflicted with selfish nodes. For provide incentives to selfish nodes, SMART uses credits. The secure multilayer credit based incentive scheme is based on the notion of layered coin. The layered coin is provides the virtual electronic credits and it is composed of various multiple layers. Each layer is produced by the source or intermediate or destination node.

## 8. SLAB

SLAB stands for Secure Localized Authentication and Billing scheme for wireless mesh network [5]. SLAB scheme is used for addressing ensure of security and ensure of system performance. Also it identifies the inter-domain handoff authentication latency and roaming broker working capacity. SLAB scheme is takes the merits of the PKI architecture for construct the trust mechanism between the various wireless internet service providers and wireless internet service providers and mobile user using roaming broker. The SLAB scheme is classified into five components. (1) Local user accounting profile (LUAP). (2) D-coin issuing and inter-domain handoff authentication phase. (3) Localized LUAP transfer during intra-domain handoff phases. (4) Clearance phase. (5) D-coin signing key distribution phase. The D-coin issuing and inter-domain handoff authentication phase is performed in on-line while mobile user handoffs. Other phases such as LUAP, localized LUAP transfer during intra-domain hand-off phase, clearance phase, D-coin signing key distribution phase are done for the managing and servicing of the handoff events.

## 9. SPARK

SPARK is stands for new VANET- based Smart PARKing scheme for large parking lots [13],[11],[15]. VANET is stands for Vehicle Ad hoc Networks. SPARK is done via vehicular communication. Real-time parking navigation service, intelligent anti-theft protection and friendly parking information dissemination are provided with drivers using SPARK. SPARK provides the drivers with easy parking services in a huge level parking. In the real-time parking navigation, the drivers can easily and fast search free parking space. Therefore, wasting of time can be reduced. In intelligent anti-theft protection scheme, every vehicle is parked in smart place which are guarded by the roadside units. The detection of the theft can be easily and quickly done by the roadside units. In the friendly parking information dissemination service, a perfect parking which is close to the destination place is choose by the drivers in a comfortable way. In the conditional privacy preservation, the real identifier ID must be kept secret when a vehicle enters in a smart parking. The bilinear paring technique is the basis of the SPARK scheme. SPARK scheme can reduce the wasting of time while searching the parking place and wasting of fuels.

## 10. BLACKHOLE ATTACK

Blackhole attack is similar to the packet drop attack [4]. It is a type of denial of service (DOS) attack. The blackhole is the place in the network where receiving or sending traffic is discarded without the knowledge of the source that the data did not reach the destination place. Generally, the blackhole attack is present in the Mobile Ad hoc networks (MANET). Blackhole problem in mobile ad hoc network is a security problem which is to be solved. In the blackhole attack, malicious node use the routing protocol to advertise itself for having the shortest path to the packet which it wants to send the data. There are two solution for blackhole attack. The first solution is to search more than one way to destination. The sender node requires verifying the authenticity of the node. This solution ensures to search the safe and correct route to the destination. The demerit is time delay. The second solution is to exploit the sequence number of the data packets which are consist in any packet header. The sequence number is an ascending order that is the next packet must be the bigger value than the present packet number. This solution gives a quick and reliable way to address the reply which is not related.

## 11. CONCLUSION

The conclusion intended to study and analysis of various misbehaving detection scheme, concepts and technique used in DTN. Simbet and bubble rap are used to identify some bridge nodes in the network using betweenness centrality and similarity metrics. The watchdog is used for detect and isolating misbehaving nodes. The pathrater combines the link reliability with knowledge of misbehaving nodes. The practical incentive protocol (Pi) is used for address the selfishness problem in DTN. A secure multilayer credit-based incentive scheme (SMART) uses credits for provide incentives to selfish nodes in the network. A secure localized authentication and billing scheme for wireless mesh network (SLAB) is used for addressing the ensure of security and performance of the system. A new VANET-based smart parking scheme for large parking lots (SPARK) is used for easy parking services in large parking lots. The blackhole attack is mainly used for controlling the traffic. The future work will be implemented using trusted authority scheme in Delay tolerant network (DTN). It is mainly used for developing a robust trust mechanism. And it is for detecting the misbehavior nodes in delay tolerant network.

## 12. REFERENCES

[1] A. Garyfalos and K. C. Almeroth, "Coupons: A multilevel incentive scheme for information dissemination in mobile networks," IEEE Trans.Mobile Comput., vol. 7, no. 6, pp. 792–804, Jun. 2008.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Lecture Notes Computer Sci., Advances Cryptology -CRYPTO 2001, vol. 2139. Springer-Verlag, 2001, pp. 213-229.

[3] E. M. Daly and M. Haahr, "Social network analysis for routing indisconnected delay-tolerant manets," in ACM MobiHoc, 2007.

[4] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM '09, 2009.

[5] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.

[6] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: a secure multilayer credit based incentive scheme for delay-tolerant networks," IEEE Trans. Veh. Technol, vol. 58, no. 8, pp. 4628-4639, 2009..

[7] J. Burgess, G. Bissias, M. Corner, and B. Levine. Surviving attacks on disruption-tolerant networks without authentication. In Proc. of ACM MobiHoc, 2007.

[8] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay tolerant networks," in ACM MobiHoc, 2008..

[9] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputationbased incentive scheme for ad hoc networks," in Proc. WCNC, Atlanta,GA, Mar. 2004, pp. 825–830.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communitions,"in Proc. 27th Conf. Computer Commun. (INFOCOM 2008),Phoenix, AZ, USA, Apr. 2008, pp. 1229-1237..

[11] R. Panayappan, J. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in Proc. of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2007), Montr´eal, Qu´ebec, Canada, pp. 75-76, Sept. 2007.

[12] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical IncentivProtocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010

[13] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.

[14] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACMMobiCom '00, 2000.

[15] Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing (RAR) in vehicular networks", in Proc. IEEE ICC 2006, Vol. 8, pp. 3602-3607,

[16] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," Wirel. Netw., vol. 13, no. 5, pp. 569–582,Oct. 2007. Istanbul, Turkey, June 2006.