INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

A Survey of Packet Dropper Detection in Wireless Network

Swati Patil
G. H. Raisoni Institute of Engineering & Management, Jalgaon, India
Ashwini Gawande
ME (CSE), G. H. Raisoni Institute of Engineering & Management, Jalgaon, India

Abstract:
Mobile ad hoc network is set of nodes which build network dynamical for exchanging information over a multi hop wireless communication .In MANET free travelling of misbehavior or packet dropper nodes is most important matter for the organization and survivability of self-organized network. The misbehavior of this node affects the performance of network. Different techniques are proposed by the researchers to mitigate this misbehavior. In this paper we study some of the important work carried out in mitigating misbehavior of packet dropper node and providing comparison between the different proposed methods.

***Key words**: Mobile Ad Hoc network, Packet dropping, Mobile node, Packet forwarding, Mitigating*

1. Introduction

Mobile Ad Hoc Network is set of nodes which builds a network in which nodes moves without need for any basic infrastructure for establishing communication between mobile nodes are forwards over a multi hop wireless links. The MANET is used in different area for different purpose. In such network nodes are belonging to different group of people so that each time they are not co-operate properly for packet forwarding in network some of the nodes do not wish to forward the packet in order to save its own resources like battery power, bandwidth etc.[17].

The advantage of wireless communication technology is less expensive. The nodes are free to move arbitrarily so that, network topology may change quickly and suddenly. Some of the proposed system used a Dynamic Source Routing (DSR) for establishing path from source to destination over a network .

IEEE 802.11 DCF MAC Protocol was designed to provide a reasonable performance in a two hop ACK[15][16]. In this security is required such as 1) confidentially i.e network should ensure that the given message is not understand by other recipients.2) Authentication i.e the data is received and send by authenticated users only. 3) Availability i.e provide required services to authenticated users when it is expected .4) Integrity i.e system should ensure that message send from the sender is received by the receiver without any modification during transaction.[16][17].

Ad Hoc networking achieving popularity with the recent production of mobile computers. So that Ad Hoc networking become a challenging task

In this Paper we review a different packet dropper detection techniques proposed by the researchers. Packet dropper nodes are those who are not interested forwarding nodes. For e.g. suppose A, B, C, D nodes are presents in network. Source node A wants send Message to node D. Node A Send message via node B and node C. This node A Forward Packet to node B.Node B accept it and forward received ACK .Node B forward packet to node C .Node C accept packet but not interested forward packet to neighboring node. So, packet is not delivered to destination .So that, node C is misbehavior or packet dropper node.

2. Misbehavior or Packet Dropper Mitigation

Most of the works to mitigate misbehavior can be classified into Credit-Based System, Reputation-Based System and Acknowledgement base System. Below describes the different techniques proposed by researchers for detection of packet dropper or misbehavior.

2.1. Credit-Based System

Credit-Based System [8] proposed by L. Buttyan et al., this system is designed to provide incentives for forwarding packet. In proposed system nodes receives credit for each packet they forward and spend their collected credit to transmit their own packet.

The Nuglet [2] is most reputed work in this category. This is done through the use of counter which is called nuglet counter. Tamper proof hardware module used for implement nuglet counter. This module is known as security module. This security module is used to provide universal protection from software and physical attacks. Nuglet counter maintain by security module when node forwards a packet the nuglet counter is incremented each time by one and when node transmits its own packet it decremented each time by one. The nuglet counter should take a positive value and cannot be arbitrarily changed by node. So that, this system ensures that the packet dropper nodes does not earn enough nuglet to send its own packet.

Zhong et al. [9] proposed Sprite, in which nodes collect receipts for the packets that they forward to other nodes. For a packet sent from a source to a destination, each node along the path records a hash of the packet as the receipt, and forwards the packet to its next hop. When the node has a high-speed link to a Credit Clearance Service (CCS), it uploads its receipts. The CCS determines the value of the receipts and provides credit in exchange. Credit is only granted if the destination reports a receipt verifying reception of the packet and if the node was on the routing path. Once verified, credit is removed from the sources account and given to each node who participated in packet forwarding. Thus nodes that transmit their own packets but do not cooperate in packet forwarding will incur a debt at the CSS. Debt accumulation beyond a certain threshold is interpreted as misbehavior.

Crowcroft et al. [6] proposed a scheme which not only rewards nodes for participating in packet forwarding with credit, but takes into account congestion and traffic flow. When sending a packet, the source computes a congestion price, which is a metric defined by the required power for transmission and the available bandwidth. It then compares this price to its personal willingness-to-pay parameter, which the source continually adjusts, based on its personal observations. By taking into consideration bandwidth in computing the cost (credit) required to send a message to the destination, the scheme avoids overwhelming low cost routes, as they would increase in costs as they become saturated. Power and bandwidth metrics are dynamically updated based on shared information among nodes.

Salem et al. [19] proposed a scheme to provide incentives to nodes in multihop cellular networks. The scheme relies on the fact that all network traffic must travel through the base stations (i.e. cell towers), and that all base stations are owned by a single trusted operator. When the source sends a packet, it appends a keyed hash of the entire packet. Each intermediate node re-hashes the entire packet, including the previously appended hash. The previous node's hash is then replaced with the new intermediate hash. Once at the base station, the hash is verified and the packet is transmitted over the backbone network, where it is re-transmitted to the destination from a nearby base station. The source is charged immediately by the base station upon receipt of a packet, while the destination is charged a small amount when the packet is re-transmitted. This amount is refunded once the destination acknowledges the reception of the packet, thus preventing the destination from cheating the system by claiming packets were never received. While credit-based systems motivate misbehaving nodes to cooperate in packet forwarding, they provide no incentive to malicious nodes that target the network throughput. Such nodes have no incentive to collect credit and receive no punishment for non-cooperation. Sprite does not require tamper proof hardware.

2.2. Reputation-Based System

Reputation-based systems use neighborhood monitoring techniques to identify misbehaving nodes. S.Mark et al.[1] proposed method which relies on two tools the watchdog and path rater. These tools are implemented on the top of Dynamic Source Routing(DSR).The watchdog module implemented by maintaining buffer of recently sent packet and comparing each overhead packet with the packet in the buffer to see if there is a match. The watchdog module monitors the behavior of their next hop node. Once a node forwards a packet to the next hop, the node overhears to verify that the next hop node faithfully forwarded the packet. If packets remain in the each longer than a threshold period. The watchdog makes an accusation of misbehavior. The main limitation of this method is that may not detect a misbehaving node in presence of ambiguous collision, receiver collisions, limited transmission power, false misbehavior, collision and partial dropping

Buchegger and Le Boudec [4] proposed a scheme called CONFIDANT, which is built upon the watchdog/path rater model. Nodes perform neighborhood monitoring using their radios in promiscuous mode while selecting paths that attempt to avoid misbehaving nodes. Whereas Marti et al. proposed using only the previous hop for monitoring, CONFIDANT requires all neighboring nodes to operate in promiscuous mode for monitoring, thus replying on a neighborhood watch. In addition, monitoring nodes notify other nodes of detected misbehavior through the broadcast of alarm messages. Instead of including a proof of the misbehavior in the alarm message, a scheme based on Pretty Good Privacy (PGP) is implemented to determine the trust level of the alarm message.

Soltanali et al. [14] propose a reputation-based scheme consisting of four modules: a Monitor, a Opinion Manager, a Reputation Manager, and a Routing/Forwarding Manager. The Monitor module monitors the nodes neighbors via the watchdog model, verifying that neighboring nodes faithfully participate in packet forwarding. Based on observations from the Monitor, the Opinion Manager formulates opinions of the nodes behavior and periodically advertises them to neighboring nodes. The Reputation Manager accepts these opinions and processes them to arrive at a trust metric for a specific node. When establishing a routing path to a destination, the Routing/Forwarding Manager uses these trust metrics to avoid including untrustworthy (misbehaving) nodes.

Paul and Westhoff [5] proposed a scheme which can identify different types of misbehavior through routing message verification and packet comparisons. In particular, they focus on securing DSR to attacks, in which a misbehaving node either (a) refuse to forward route request packets, (b) forwards route requests without adding itself to the routing path, or (c) adds unrelated nodes to the route request. The scheme verifies routing messages through the use of an un-keyed hash chain, while nodes compare RREQ headers to a local cache consisting of headers from overheard packets to identify misbehavior. Each intermediate node along the path thus monitors its neighboring nodes, and sends any accusations of misbehavior to the source, along with the type of misbehavior they witnessed. The source analyzes all accusations received, and takes action based on the type of misbehavior witnessed.

Michiardi and Molva [19] proposed CORE, in which nodes create a composite reputation rating for a given node by combining the nodes subjective reputation, its indirect reputation and its functional reputation. The subjective reputation is calculated from direct observation of the nodes behavior, using a weighted average of both current and past observations. The indirect reputation is a value calculated based on second-hand observations made by other nodes in the network. A node's functional reputation is based on task-specific behavior. Thus it is computed based on its reputation in packet forwarding, routing, etc. Denial-of-service attacks based on misbehaving nodes broadcasting negative ratings for honest nodes are prevented by preventing nodes from broadcasting negative behavior. Thus when sharing reputation metrics, node are restricted to sharing only positive ratings.

2.3. Acknowledgement-Based System

Acknowledgment-based systems [3, 7, 11, 13, 16] rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. Balakrishnan et al. [11] proposed a scheme called TWOACK, where nodes explicitly send 2-hop acknowledgment messages (TWOACK) to verify cooperation. For every packet a node receives, it sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior. TWOACK can be implemented on top of any source routing protocol such as DSR.

Liu et al. [13] improved on TWOACK by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. Additionally, 2ACK uses a one-way hash chain to allow nodes in the routing path to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Padmanabhan and Simon [7] proposed a method called secure trace route to identify the link on which misbehavior is occurring. Instead of the standard trace route operation, which relies on nodes responding to expired packets, secure traceroute verifies the origin of responses and uses traceroute packets that are indistinguishable from data packets. Secure traceroute proceeds hop by hop, although instead of responding to expired packets, the source establishes a shared key with the node. By encrypting the packets, secure traceroute packets are indistinguishable from data packets and cannot be selectively dropped. A Message Authentication Code (MAC) is utilized for authenticating the packets origin. Although traceroute is considered a reactive approach, secure traceroute is proactive, requiring connected nodes to transmit \keep-alive" packets when they have data to send.

Awerbuch et al. [3] proposed an on demand routing protocol that probes the path to identify the faulty link. Once misbehavior is identified as occurring, the source begins probing nodes on the routing path by asking nodes to acknowledge all packets received. Probing is performed according to a binary search, in which the binary response of probed nodes is failed, successful. Once the faulty link has been identified, a weight metric is utilized to increase the value of the faulty link, thus avoiding including it in future routing paths. To avoid a misbehaving node from dropping the acknowledgments of probed nodes, the acknowledgment are attached to packets from previous nodes such that the misbehaving node cannot drop only a subset of acknowledgment messages. The source makes no attempt to identify the individual node(s) causing the misbehavior.

Mehdi Keshavarz and Mehdi Dehghan [16] proposed approach categorized as Detection and Punishment-based approach. In this approach, we use *overhearing of MAClayer acknowledgments* as a novel detection tool to detect misbehaving data packet-dropper nodes. This system describes and analyzes our technique as an add-on for Dynamic Source Routing (DSR) protocol. In this system misbehavior detected when forwarder node on a source route sends back a MAC-layer ACK for a received data packet that should forward it, this ACK packet can both be *received* by the transmitter of related data packet and be *overheard* by all nodes in the transmission range of both ACK-transmitter and its successor node on the source route.

Acknowledgment-based systems are proactive, and hence incur message overhead regardless of the presence of misbehavior. 2ACK provides a method to reduce message overhead by acknowledging only a fraction of the packets, with the tradeoff of increased delay in misbehavior detection. Awerbuch et al. further reduces overhead through its on demand characteristic, however it only identifies the faulty link, thus failing to identify the node causing the misbehavior.

3. Conclusion and Future Scope

In this paper, we study various systems for detect and prevent misbehavior of node proposed by researchers. The work is classified into Credit-based system, Reputation-based system and Acknowledgement-based system. In this paper we study different solutions proposed to detect and isolate the misbehavior of mobile nodes. Which helps to improve the network performance significantly? The comparison of proposed work helps us to find the limitations and advantages of the system. We conclude that most proposed system have their own limitations.

During the survey, we also find some points that can be further explored in the future, we find some systems are really better. We will try to explore deeper in this research area.

In future we will use other types of routing protocol. So that our technique can work effectively MANET, by adding different techniques it will become more interesting.

	Design	Computational Overhead	Communication Overhead	Punishment	Routing Protocol
L. Buttyan [8]	Stand-alone	Low	Low	Yes	DSR or AODV
Nuglets [2]	Stand-alone	Low	No	Yes	DSR or AODV
Sprite [9]	Centralized	Medium	Medium	Yes	DSR
Watchdog [1]	Distributed	Low	No	No	DSR
CORE [19]	Distributed	Low	Low	Yes	DSR
CONFIDANT [4]	Distributed	Low	Low	Yes	DSR
TWOACK[11]	Stand-alone	Low	High	Yes	DSR
2ACK [13]	Stand-alone	Low	Low	No	DSR
Mehdi Keshavarz[16]	Stand-alone	Low	High	Yes	DSR

Table 1: A summary of the characteristics of the Surveyed Schemes

4. References

1. S. Marti, T. Giuli, K. Lai, and M. Baker. “Mitigating routing misbehavior in mobile ad hoc networks,” In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), pages 255-265, 2000.
2. L. Buttyan and J.-P. Hubaux, “Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks,” Technica Report DSC/2001/001, EPFL,Lausanne, CH, Jan. 2001.
3. B. Awerbuch, D. Holmer, C.-N. Rotaru, and H. Rubens. “An on-demand secure routing protocol resilient to byzantine failures, “In Proceedings of the ACM Workshop on Wireless Security (WiSe'02), 2002.
4. S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol,” In Proc. of MobiHoc 2002, Lausanne, CH,June 2002.
5. K. Paul and D. Westhoff. “Context aware detection of sel_sh nodes in dsr based ad-hoc networks,” In Proceedings of the IEEE Globeco Conference, 2002.
6. J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring.“Modelling incentives for collaboration in mobile ad hoc Networks,” In Proceedings of WiOpt03, 2003.
7. V.-N. Padmanabhan and D.-R. Simon. “Secure traceroute to detect faulty or malicious routing,” SIGCOMM Computer Communication Review, 33(1), 2003.
8. N. Salem, L. Butty_an, J. Hubaux, and M. Jakobsson. “A charging and rewarding scheme for packet forwarding in multi-hop cellular networks,” In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pages 13-24. ACM New York, NY, USA, 2003.
9. S. Zhong, J. Chen, and Y.-R. Yang, “Sprite: A Simple, Cheat- Proof Credit-Based System for Mobile Ad-Hoc Networks,” In Proc. of IEEE INFOCOM’03, pp. 1987-1997, San Francisco USA, Mar. 2003.
10. D. B. Johnson, D. A. Maltz, and Y. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR),” IETF Internet Draft, draft-ietf-manet-dsr- 10.txt, Jul. 2004.
11. K. Balakrishnan, J. Deng, and P. K. Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,” In Proc. of IEEE WCNC 2005, New Orleans, LA, USA, Mar. 2005.
12. L.Buttyan and J.-P. Hubaux, “Security and Cooperation in Wireless Networks,” http://secowinet.epfl.ch/, 2006.
13. K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. “An acknowledgmentbased approach for the detection of routing misbehavior in manets,” IEEE Transactions on Mobile Computing, 6(5):536- 550, May 2007.
14. S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei.“An Efficient Scheme to Motivate Cooperation in Mobile Ad hoc Networks,” In Proceedings of the Third International Conference on Networking and Services, pages 98-98, 2007.
15. LAN/MAN Standards Committee of the IEEE Computer Society, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” pp. 1-1233, June. 12, 2007.
16. Mehdi Keshavarz, Mehdi Dehghan “MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks,” Computer Eng. Department Islamic Azad University Qazvin, IRAN, 2012

17. Mani P., Kamalakkannan P.”Mitigating Selfish Behavior in Mobile Ad Hoc Networks: A survey,”In IJCA(0975-8887,volume73-No.22,July2013
18. Reeta Bourasi, Prof Sandeep Sahu “Detection and Removal of Packet Dropper Node for Congestion Control Over The MANET,”International Journal of Innovation Research in electrical, Electronic, Instrumentation and Control Engineering Vol. 1, Issue 2, May 2013
19. P. Michiardi and R. Molva. “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” In Proceedings of the Sixth IFIP Conference on Security Communications and Multimedia (CMS02), 2002