Monitoring the Misbehaving Nodes in MANET using Audit-Based Misbehaviour Detection (AMD) Method

S.Alagumuthukrishnan[1], Dr.K.Geetha[2], J.Blessy Achsah[3] and A.Ancy Mary[4]

[1]*Department of Computer Science and Engineering, RVS College of Engineering and Technology, Coimbatore. Email:alagumuthukrishnan@gmail.com*
[2]*Department of Electrical and Electronics Engineering, Karpagam Institute of Technology, Coimbatore. Email: geetha.arulmani@gmail.com*
[3]*Department of Computer Science and Engineering, RVS College of Engineering and Technology, Coimbatore. Email: achsahjeyakumar@gmail.com*
[4]*Department of Computer Science and Engineering, RVS College of Engineering and Technology, Coimbatore. Email: ancymary7007@gmail.com*

Article Received: 27 March 2017 *Article Accepted: 07 April 2017* *Article Published: 11 April 2017*

ABSTRACT

In MANET, the mobile nodes within radio range can directly communicate, whereas others need the help of intermediate nodes to forward their packets. As nodes themselves are participating in exchanging the messages, any selfish node in the network can easily misuse the message traffic by dropping messages or by generating false messages. Here the misbehaving nodes that refuse to forward packets in multi-hop ad hoc networks are addressed. We have used a system called Audit-Based Misbehaviour Detection (AMD) that isolates both continuous and selective packet droppers. The AMD system achieves per-packet behaviour evaluation. Here we have enabled Watchdog. It detects the misbehaving nodes in the networks. Thus the result is shown via simulations that AMD successfully identifies the misbehaving nodes.

Keywords: MANET, Misbehaving nodes, Packet dropping and Watchdog.

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network. As the nodes move from (or move within) the transmission range of other nodes, the resulting change in network topology dynamically changes the current routing information in each node (removing, updating valid routers). As no centralized core network exists within MANETs, additional robustness against single failure is an advantage. Mobile ad-hoc network is chosen as it involves setting up fixed access points and in places where infrastructure is not always possible, destroyed or impractical. Also it is easy to deploy. AMD provides a comprehensive misbehaviour identification and node isolation system for eliminating misbehaviour from a given network. AMD enables the per-packet evaluation of a node's behaviour without incurring a per-packet overhead. Watchdog detects the selfish nodes in the networks. Collaborative watchdog indicates the presence of the selfish node to the source node. If the watchdog detects a selfish node, it is marked as positive detection or negative detection. This approach reduces the detection time.

2. RELATED WORKS

The concept of mobile ad-hoc networks and its security issues was carried out by many researchers. This section describes the detection of misbehaving nodes on mobile ad-hoc networks. *Jian-Ming Chang et al., (2015),* presented the paper "Defending against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach". In this context, preventing or detecting malicious nodes launching gray hole or collaborative black hole attacks is a challenge. This paper resolved this issue by designing a DSR routing mechanism, which is referred to as the Cooperative Bait Detection Scheme (CBDS) combines the advantages of both proactive and reactive defense architectures. Reverse tracing technique is used to achieve the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks. *Shishir K. Shandilya et al., (2010)* presented the paper "A Trust-Based Security Scheme for RREQ Flooding Attack in MANET".The effectiveness of the proposed technique depends on the selection of threshold values. The concept of delay queue reduces the probability of accidental blacklisting of the node but it also delays the detection of misbehaving node by allowing him sends more packet until delay queue time out occurs. *Yoav Sasson et al., (2003)* have proposed "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks". The plain flooding algorithm provoked a high number of unnecessary packet rebroadcasts, causing contention, packet collisions and ultimately wasting precious limited bandwidth. And they had explored the phase transition phenomenon observed in percolation theory and random graphs as the basis for defining probabilistic flooding algorithms. By considering ideal and realistic models, a better understanding of the factors that determine phase transition was acquired.

3. PROBLEM DEFINITION

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc networks. Continuous packet dropping can effectively degrade the performance of the network. Monitoring operations must be repeated on every hop of a multi-hop route, thus leading to high communication overhead and energy expenditure.

4. SYSTEM DESCRIPTION

4.1. Existing Method

Cooperative Bait Detection Scheme (CBDS) is used to detect malicious nodes launching collaborative attacks in MANET.By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and by reverse tracing program it detects the malicious nodes and consequently prevent the attacks.

4.2. Proposed Method

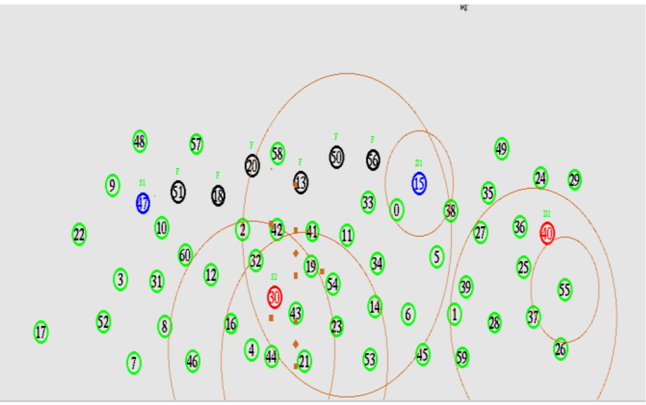
Audit-Based Misbehavior Detection (AMD) achieves per-packet behavior evaluation without incurring a per-packet per-hop cost.AMD integrates three critical functions: reputation management, trustworthy route discovery and identification of misbehaving nodes via behavioral audits**.** Watchdog detects the selfish nodes in the networks. Watchdog reduces the detection time and improves the precision by reducing the effect of both false positives and false negatives.

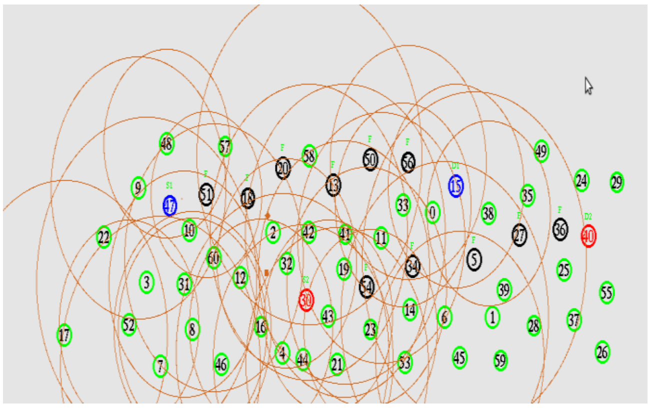
5. SYSTEM MODELING

In this paper we are going to detect the misbehaving nodes in MANET using Audit-based Misbehaviour Detection Method which achieves per-packet behavior evaluation. The system is modeled into following three categories:

A. *Reputation Module*

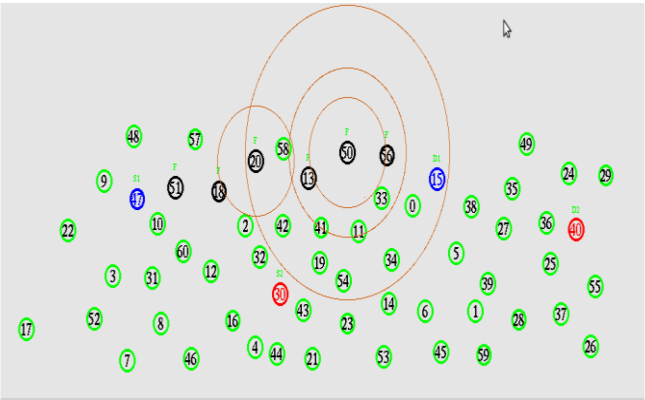
The reputation module is responsible for computing and managing the reputation of nodes. It adopts a decentralized approach in which each node maintains its own view of the reputation of other nodes on the basis of firsthand information or second hand information. Such implementation make easier the communication overhead for transmitting information to a centralized location and translates to the distributed nature of wireless ad hoc networks.





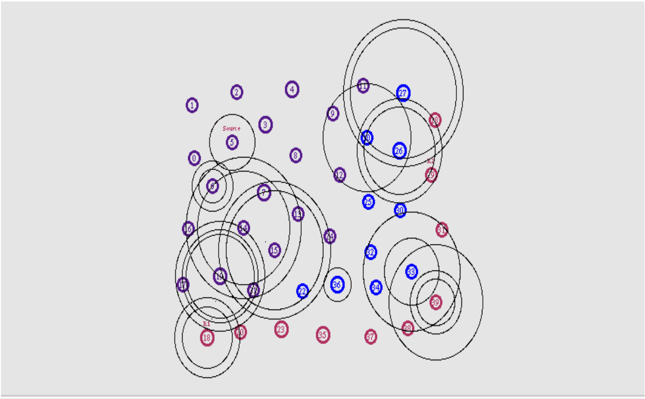
B. Route Discovery Module

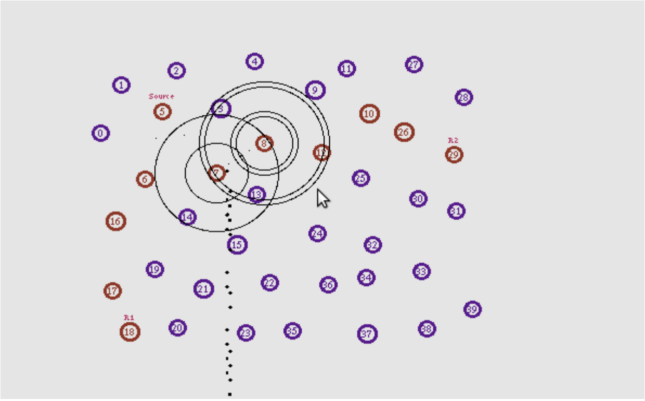
The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination. The reputation values are individual perceptions of trustworthiness of one node in regards to another.

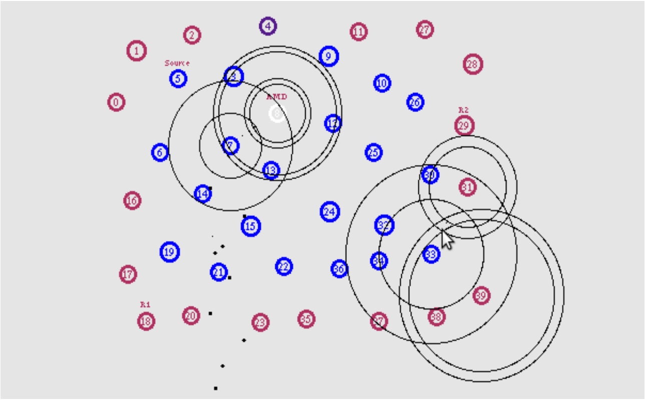


C. Audit Module

The audit module efficiently and quickly identifies misbehaving nodes by an audit process. This process is accelerated based on input received from the reputation module.







6. SYSTEM ARCHITECTURE

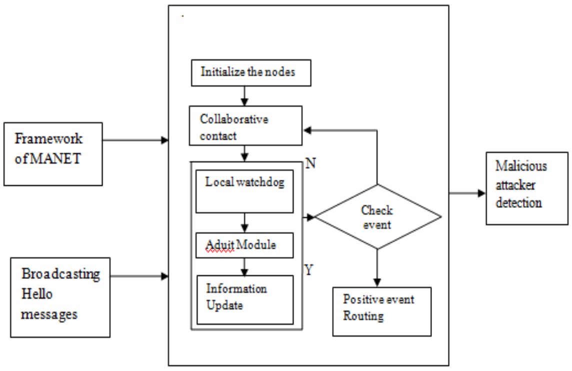


Fig.1. Architecture of Message Passing Using AMD

In Fig1., the Hello message is broadcasted to the nodes in the network. Here, first we initialize the nodes. A contact is done which is an opportunity of transmission between a pair of nodes i.e., two nodes have enough time to communicate. Then the local watchdog is used to detect the selfish nodes in the network. It informs to the neighbour node that there is a misbehaving node. . When the neighbour node receives a message, it generates an event to the network information module with the list of positive and negative detections. The Audit module checks the list and the information is updated. Finally the misbehaving nodes are detected by initiating the message process by means of ***rreq*** and ***rrep*** process. The basic operation of source S to destination D through the intermediate nodes of B and C are performed and it is shown below:

MESSAGE PROCESS

Route request *(rreq)* process:

- Initiator node
  - Initiate a *rreq* to target
  - Intermediate nodes
    - previously seen *rreq*→ take no action
  - Else
    - If not target → append id to path and retransmit *rreq*
    - If target → take actions below in rrep

Route reply *rrep* process:

- Target node
  - Calculate and attach signature over the path in the received *rreq*
  - Unicast the *rrep*
- Intermediate nodes (along the unicast path)
  - If not initiator
    - Calculate and attach signature over the received *rrep*
    - Transmit updated *rrep* to next upstream` host
  - If initiator
    - Validate the accumulated path against the target signature
    - Validate individual signatures to ensure that every node in target signature has supplied a signature in the reverse path order

BASIC OPERATION:

S → *: (rreq, S, D, *id*, ())
B → *: (rreq, S, D, *id*, (B))
C → *: (rreq, S, D, *id*, (B, C))
D → C: (rrep, S, D, (B, C), (*sig*D))
C → B: (rrep, S, D, (B, C), (*sig*D, *sig*C))
B → S: (rrep, S, D, (B, C), (*sig*D, *sig*C, *sig*B)

7. SIMULATION RESULTS

In this section, the simulations are carried out by considering with some parameters and values respectively. Here the simulation tool NS2 is used to generate the simulation according to the parameter specification for 40 nodes. Also various performance metrics are taken and their comparison graphs are obtained.

Table 1.Simulation Parameters

Parameters	Value
Channel type	Wireless
Message port	42
Propagation	Two Ray Ground
Routing protocol	AODV
Area	1500*500
Traffic	CBR
Channel data rate	11Mbps
Antenna type	Omni Antenna

Performance Metrics:

I. Packet Drop:

It occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion.

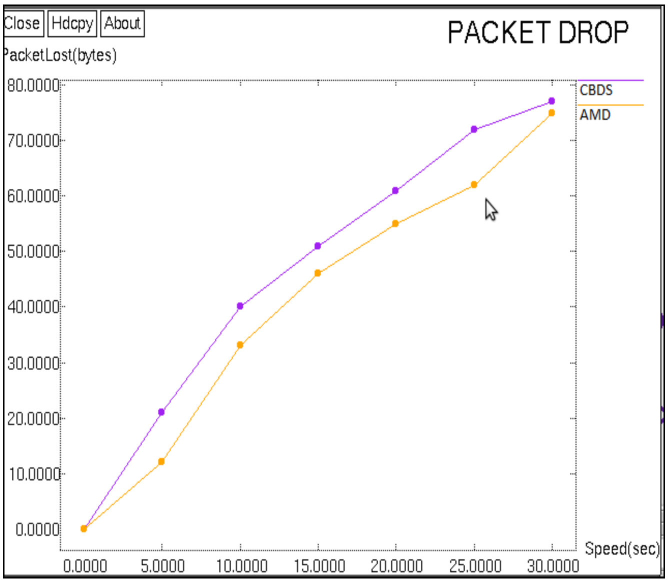


Fig.2. Graph for Packet Drop Variations

II. Throughput:

This is defined as the total amount of data that the destination receives them from the source divided by the time it takes for the destination to get the final packet.

$$T=1/n \sum_{i=1}^{n} b_i/t_i$$

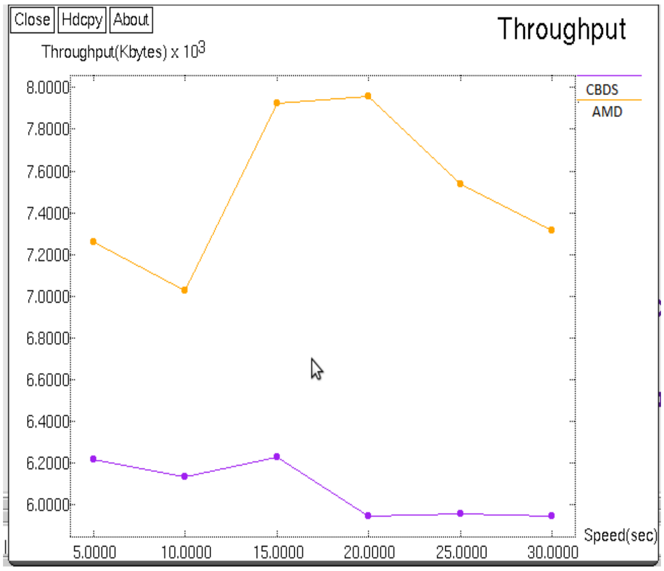


Fig.3. Graph for Throughput Variations

III. End -to-End Latency:

This is defined as the average time taken for a packet to be transmitted from the source to the destination.

$$E=1/n \sum_{i=1}^{n} d_i/pktd_i$$

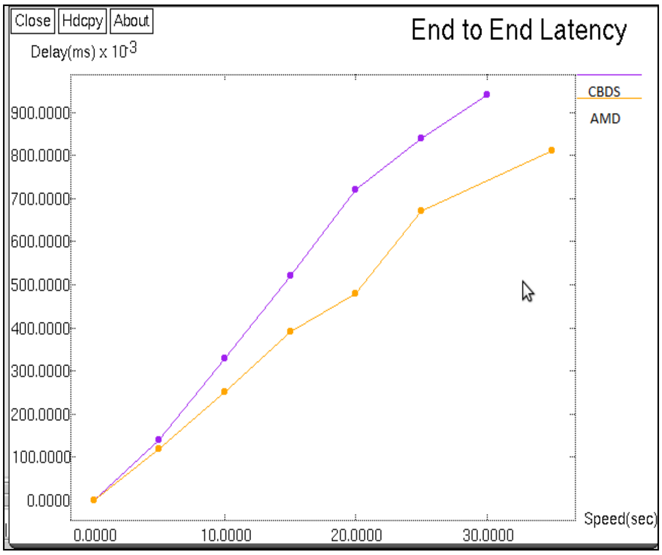


Fig.4. Graph for End to End Latency

IV. Packet Delivery Ratio:

This is defined as the ratio of number of packets received at the destination and the number of packets sent by the source.

$$PDR=1/n \sum_{i=1}^{n} pktd_i/pkts_i$$

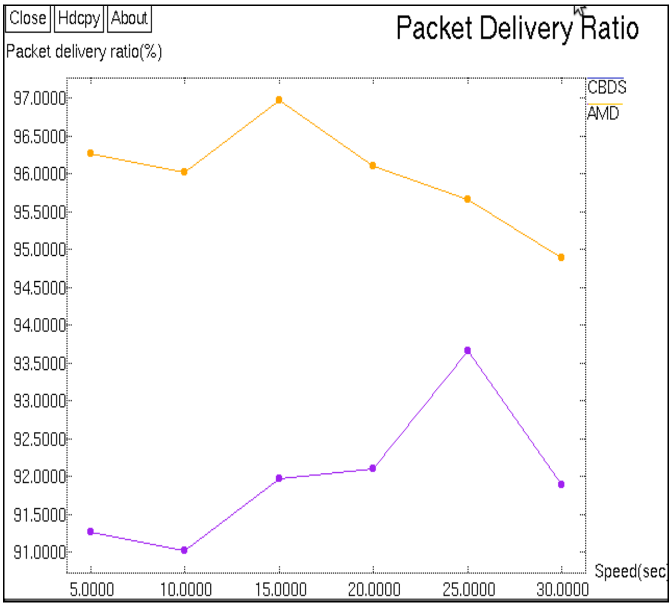


Fig.5. Graph for Packet Delivery Ratio

V. Energy Consumption:

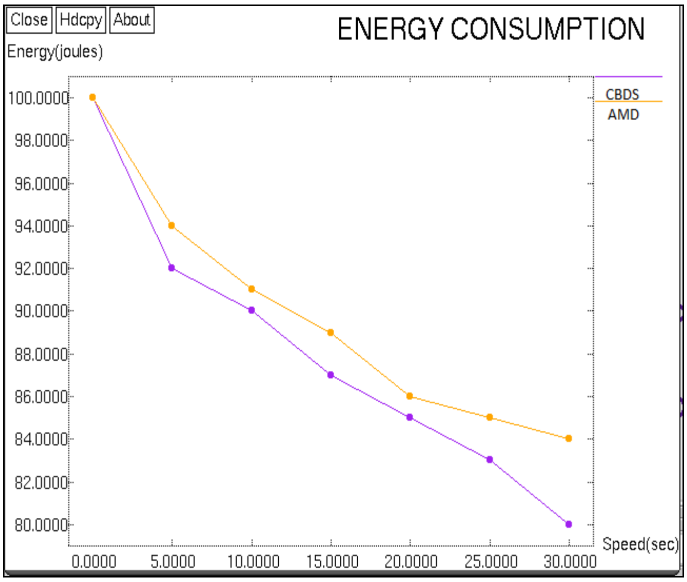


Fig.6. Graph for Energy Consumption

8. CONCLUSION AND FUTURE WORK

In this paper we used AMD which integrates three critical functions such as reputation management, route discovery and identification of misbehaving nodes via behavioural audits. AMD recovers the network operation even if a large fraction of nodes is misbehaving at a lower communication cost. The future work could be carried out in large-scale by using any new detection technique to detect the misbehaving nodes in MANET and reduce the communication overhead at each nodes with low cost.

REFERENCES

[1] P-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture”.

[2] S. Corson and J.Macker, Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. *(Last retrieved March 18, 2013). [Online]. Available:http://www.elook.org/computing/rfc/rfc2501.html*

[3] C. Chang, Y.Wang, and H. Chao, “An efficient Mesh-based core multicast routing protocol on MANETs”.

[4] D. Johnson and D. Maltz, “Dynamic source routing in Adhoc wireless networks,” *Mobile Computing.*, pp. 153–181, 1996.

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile- backbone protocol for ad hoc wireless networks,” in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.

[6] A. Baadache and A. Belmehdi, “Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks,” *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.

[8] K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, “An Acknowledgement based approach for the detection of routing misbehavior in MANETs,” *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[10] H. Deng, W. Li, and D. Agrawal, “Routing security in wireless ad hoc network,” *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attacks in wireless ad hoc networks,” in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[12] H. Weerasinghe and H. Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation,” in *Proc. IEEE ICC*, 2007, pp. 362–367.

[13] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments,” *Wireless Pers. Commun.*, vol. 29, pp. 367–388, 2004.

[14] W. Kozma and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in *Proc. WiSec*, 2009, pp. 103–110.

[15] W. Wang, B. Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks".