# An Energy Efficient and Secure Cooperative Bait Detection and Defense Approach in MANET's

Sahana K.
P G Scholar
SJCE, Mysore, Karnataka, India

## ABSTRACT

Because of the confinements of wired system in crisis circumstances like natural calamities, scope for wireless technology is expanded. Mobile Adhoc Networks technology provides more room for research. Due to the MANET characteristics, such as dynamic topology and infrastructure less, it can be stationed whenever and wherever required. Hence it can be used in many applications. In MANET, to establish the communication among the nodes, nodes should coadjutant to each other. Nodes may disrupt complete routing process in the presence of malignant nodes and this leads to serious security threat. In this context thwarting or detecting malignant nodes launching grayhole or collaborative blackhole attack is a challenge. This paper attempts to solve this issue by designing energy efficient and secured dynamic source routing mechanism, which is also cited as cooperative bait detection and defense scheme (CBDDS), which integrates the advantages of proactive and reactive defense architectures. Reverse tracing technique is used to achieve the stated goal. Design is simulated in the presence of malignant node attacks, the CBDDS outflanks as far as packet delivery ratio, end to end delay, throughput and routing overhead which are picked as execution measurements over the DSR and 2ACK directing convention picked as benchmarks.

## General Terms

Cooperative bait detection and defense scheme, Collaborative blackhole attacks, Detection mechanism, Dynamic Source Routing, Grayhole attacks, malicious node, malignant node, mobile ad hoc network.

## Keywords

CBDDS-Cooperative Bait Detection and Defense Scheme, BFTR-Best Fault Tolerance Routing, DSR-Dynamic Source Routing, MANET-Mobile Adhoc Networks.

## 1. INTRODUCTION

Widespread availability of mobile devices and infrastructure less property of ad hoc networks (MANETs) [1], [3] made the MANETs to be used in various decisive applications such as military crisis operations and emergency preparedness and response operations.

While receiving the data, wireless local area network is formed by cooperation of nodes with each other to forward the data packets. In MANET each node works as both host and the router [3].Though these features has advantage also includes serious drawbacks from a security point of view. Indeed, the applications impose some stringent constraints on the security of the network topology, routing, and data traffic.

For instance, impairment of the network operations occurs due to the presence and collaboration of malignant nodes which may rattle complete routing process. Plenty of research works targeted on security of MANETs, most of them deal with prevention and detection approaches to encounter individual offending nodes. In this regard, when multiple malignant nodes connive together to commence a collaborative attack, the efficacy of these approaches becomes weak, which may result in more calamitous damages to the network.

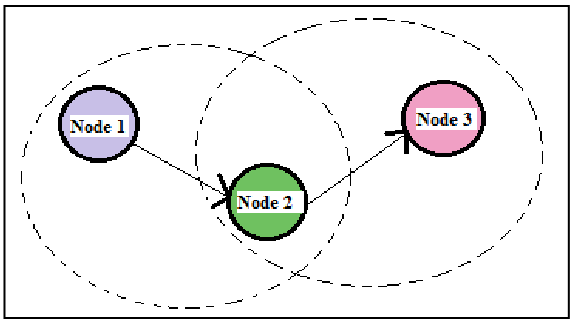


**Fig 1: Mobile Adhoc Network**

Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however, the node 2 can be used to forward packets between node 1and node 3. The node 2 will act as a router and these three nodes together form an ad-hoc network.

## 2. RELATED WORK

Several research works have investigated the problem of malignant node detection in MANETs. Most of these solutions deal with the detection of a single malignant node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks. In addition, some of these methods require specific environments [4] or assumptions to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories.1) Proactive detection schemes [5]–[11] are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage. 2) Reactive detection schemes [12]–[14] are those that trigger only when the destination node detects a significant drop in the packet delivery ratio. Among the above schemes are the ones proposed in [8] and [12], which we considered as benchmark schemes for performance comparison purposes. In [8], Liu et al. proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received.

A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes. In [12], Xue and Nahrstedt proposed a prevention mechanism called BFTR. Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path (measured in terms of packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining "good" routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect grayhole/collaborative blackhole attacks in MANETs.

## 3. PROPOSED WORK

Cooperative Bait Detection and Defense Scheme (CBDDS) is proposed, which efficiently exposes the malignant nodes that endeavor to dispatch grayhole/collaborative blackhole attacks. CBDDS uses Energy efficient dynamic source routing mechanism to find the address of an adjacent node, which can be used as bait destination address to bait malignant nodes to send a reply RREP message and malignant nodes are detected using a reverse tracing technique. Any detected malignant node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike other approaches, the CBDDS coordinates the proactive and reactive defense mechanisms to accomplish the objective.

CBDDS scheme performs its operation based on the following mechanisms:

Proactive Defense mechanism:
a) Initial bait step
b) Reverse Tracing Step

Reactive Defense mechanism:
a) Reactive Defense step

**Initial Bait Step:** The source node selects an adjacent node, i.e., nr, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ_. This is illustrated in Fig 2; Bait phase is activated whenever the bait RREQ_ is sent prior to seeking the initial routing path. The bait phase can be analyzed as follows:

First, if the nr node had not launched a blackhole attack, then after the source node had sent out the RREQ, there would be other nodes' reply RREP in addition to that of the nr node. It clearly indicates the presence of malignant node in the reply routing. The existence of malignant node in the reply routing is as shown in Fig 2. Therefore, the reverse tracing program in the next step would be initiated in order to detect this route. If only the nr node had sent the reply RREP, it means that there was no other malignant node present in the network and that the CBDDS had initiated the DSR route discovery phase.

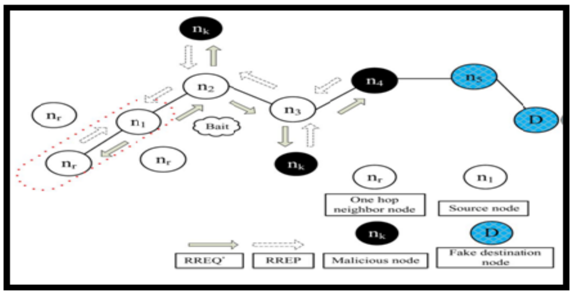


**Fig 2: Random selection of bait address [2]**

Second, if nr was the malignant node of the blackhole attack, then after the source node had sent the RREQ, other nodes (in addition to the nr node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. In this case, the reverse tracing program in the next step would be initiated to detect this route.

If nr deliberately gave no reply RREP, it would be directly listed on the blackhole list by the source node. If only the nr node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that nr had provided; in this case, the route discovery phase of DSR will be started. The route that nr provides will not be listed in the choices provided to the route discovery phase.

**Reverse Tracing Step**: The reverse tracing program is used to detect the behaviors of malignant nodes through the route reply to the RREQ_ message. If a malicious node has received the RREQ_, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDDS is able to detect more than one malignant node simultaneously when these nodes send reply RREPs.

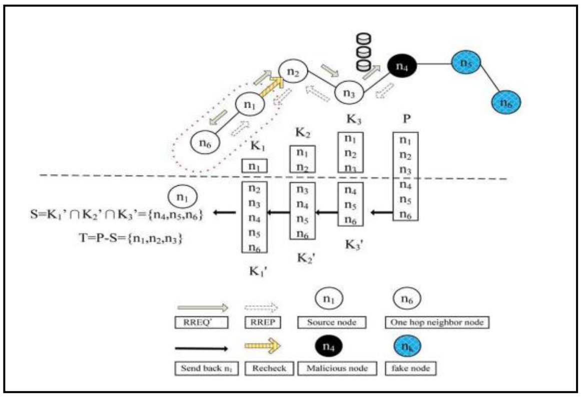


**Fig 3: Reverse tracing phase [2]**

When a malignant node, for example as shown in Fig 3, nm, replies with a false RREP, an address list P = {n1 . . . nk, nm . . . nr} is recorded in the RREP. If node nk receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list Kk= {n1, . . .nk}, where Kk represents the route information from source node n1 to destination node nk. Then, node nk will determine the differences between the address list P = {n1 . . . nk . . . nm . . . nr} recorded in the RREP and Kk= {n1 . . . nk}.

$$K`k=P-Kk= \{nk+1...nm...nr\} \qquad (1)$$

Where K`k represents the route information to the destination node.

In figure 3, n4 can reply with K`4 = {n5, n6}, n3 will check and then removeK`4 when it receives the RREP. After the source node obtains the intersection set of K`k, the dubious path information S replied by malignant nodes could be detected, i.e.

S=K`1∩ K`2∩ K`3...∩ K`k (2)

The set difference operation of P and S is conducted to acquire a temporarily trusted set T, i.e.

$$T=P-S \tag{3}$$

To confirm that the malignant node is in set S, the source node would send the test packets to this route and would send the recheck message to the second node toward the last node in T.

**Reactive Defense step:** After initial proactive defense, the DSR route discovery process is activated. When the route is established and at the destination if the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance. The threshold is a varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. A dynamic threshold algorithm is designed to control the time when the packet delivery ratio falls under the same threshold. If the time is shortened, it means that the malicious nodes are still present in the network. In that case, the threshold should be adjusted upward. Otherwise, the threshold will be lowered.

CBDDS can recognize the normal nodes by essentially taking a gander at the malignant nodes answer to each RREP. Moreover, the CBDDS is likewise fit for watching whether a malignant node would drop the packets or not. Therefore, the extent of dropped packets are neglected, and malignant nodes propelling a grayhole assault would be distinguished in an indistinguishable route from those blackhole assaults are recognized.

Principle focal points of the proposed framework are; diminished routing overhead, diminished energy utilization, diminished time delay, expanded throughput.

# 4. PERFORMANCE EVALUATION

## 4.1 Simulation Parameters

NS2 simulation tool is used to study the performance of CBDDS scheme. Source node, destination node and malignant nodes are randomly selected. Table 1 illustrates the simulation parameters used for analysis.

**Table 1. Simulation Parameters**

| PARAMETER | VALUE |
|---|---|
| MAC type | IEEE 802.11 |
| Number of nodes | 36 |
| Routing protocol | DSR |
| Maximum packet | 25 |
| Channel type | Wireless Channel |
| Initial energy | 100 |
| Initial threshold | 90% |
| Simulation time | 28ms |
| Transmission rate | 5 packets/s |
| Packet size | 256bits |
| Channel data rate | 1 Mbps |

Mathematical operations are performed to analyze proposed method. Finally, the results obtained from this module are compared against DSR [4], 2ACK schemes chosen as benchmarks and comparison X-graphs are plotted based on the following performance metrics.

**Packet Delivery Ratio**: This is defined as the ratio of the number of packets received (pktdi) at the destination and the number of packets sent (pktsi) by the source.

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktdi}{pktsi}$$

**Routing Overhead:** This metric represents the ratio of the amount of routing-related control packet (cpki) transmissions to the amount of data transmissions (pkti).

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpki}{pkti}$$

**Average End-to-End Delay:** This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is di, and the number of packets received by the destination node is pktdi

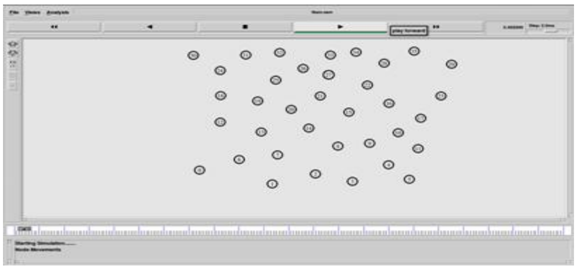
$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{di}{pktdi}$$

**Throughput:** This is defined as the total amount of data (bi) that the destination receives from the source divided by the time (ti) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second.

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{bi}{ti}$$

# 5. RESULTS

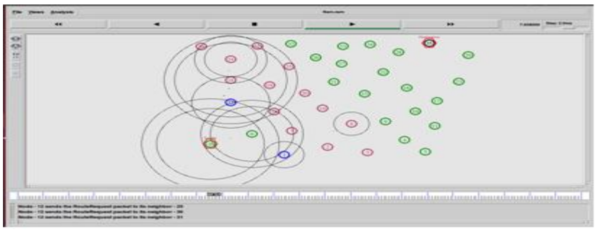
Fig 4 shows node deployment of the proposed approach. Initially nodes are moved to their respective position in the network. Totally 36 nodes are deployed by configuring network parameters.



Starting Simulation......
Node Movements

**Fig 4: Node Deployment**

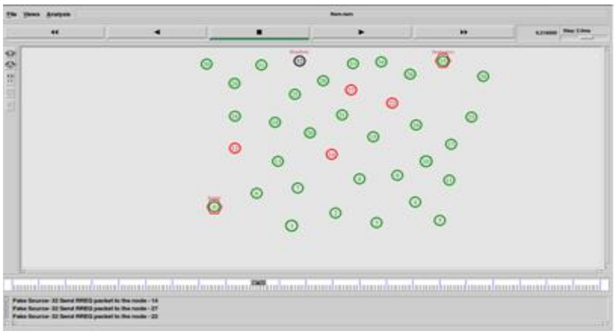
Fig 5 illustrates source node sending route request to its neighbor. In turn neighbor node will forward request to its neighbor and this process continues till it reaches destination.



```
Node - 12 sends the RouteRequest packet to the neighbor - 28
Node - 12 sends the RouteRequest packet to the neighbor - 36
Node - 12 sends the RouteRequest packet to the neighbor - 31
```

**Fig 5: Sending route request to neighbor**

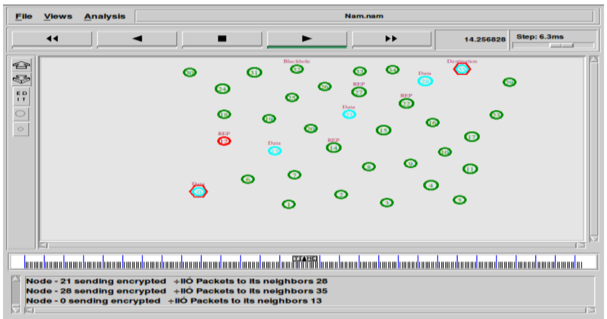
Figure 6 shows blackhole attack in which node 32 sends a fake route request to nodes 12, 14, 22 and 27. Then source node will send fake route request to its neighbors and it will get reply from node 12, 14, 22 and 27. Then shortest path is calculated.



```
Fake Source- 32 Send RREQ packet to the node - 14
Fake Source- 32 Send RREQ packet to the node - 27
Fake Source- 32 Send RREQ packet to the node - 22
```

**Fig 6: Blackhole attack**

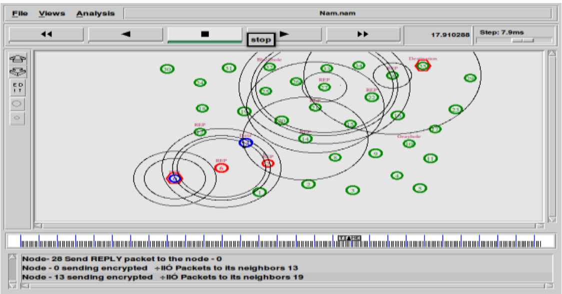
Once shortest path is calculated and network is free from malicious, encrypted packets can be transmitted to destination without any data loss. Since malicious node IP is stored in blacklist, system will reject the malicious path which is illustrated in Figure 7.



```
Node - 21 sending encrypted  +IIÓ Packets to its neighbors 28
Node - 28 sending encrypted  +IIÓ Packets to its neighbors 35
Node - 0 sending encrypted  +IIÓ Packets to its neighbors 13
```

**Fig 7: Encrypted packet transmission**

Grayhole attack can also be detected in the same way as a blackhole attack. New path is calculated; packets are encrypted and transmitted to the destination. Blue circle in figure 8 shows trusted node for packet transmission.



```
Node- 28 Send REPLY packet to the node - 0
Node - 0 sending encrypted  +IIÓ Packets to its neighbors 13
Node - 13 sending encrypted  +IIÓ Packets to its neighbors 19
```

**Fig 8: Encrypted packet transmission**

X-graph is used to analyze the performance of CBDDS over DSR and 2ACK schemes and CBDDS clearly ahead of other two schemes in terms of packet delivery ratio, routing overhead, end to end delay and throughput.

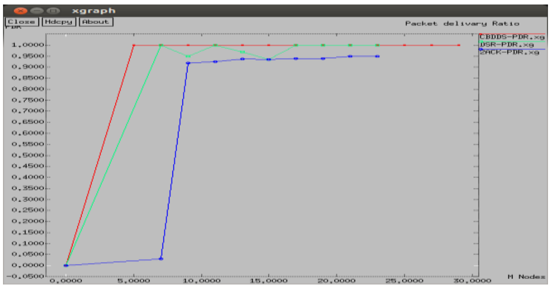


**Fig 9: Packet delivery ratio**

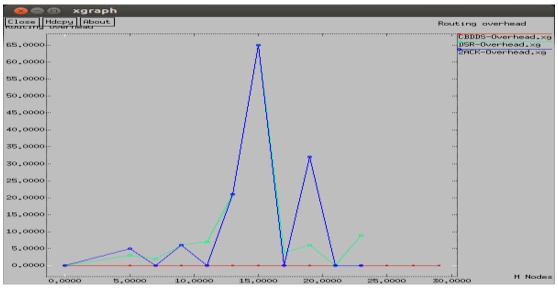


**Fig10: Routing Overhead**

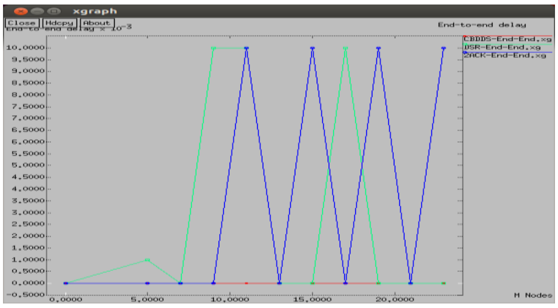


**Fig 11: End to End Delay**

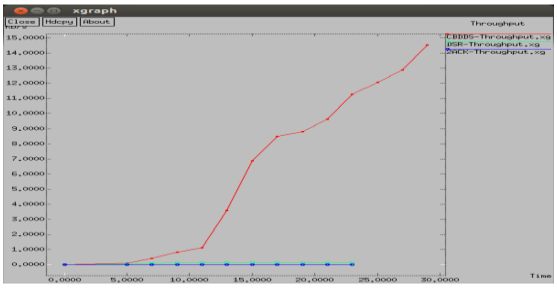


**Fig 12: Throughput**

## 6. CONCLUSION AND FUTURE WORK

Security of MANET is a major test, where routing protocols are vulnerable against grayhole and blackhole assaults. Different specialists have proposed distinctive answers for different security issues in MANETs. Proposed mechanism called as cooperative bait detection and defense scheme can be used for detecting and protecting against grayhole and blackhole attacks in MANETs. The address of an adjacent node is used as bait destination address to bait malignant nodes to send a reply message, and malicious nodes are detected using a reverse tracing technique. It uses both proactive and reactive approach to achieve its goal. A detected malicious node is kept in a blacklist so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Utilizing RSA calculation information bundles are encrypted and thus packets are sent to the goal in secure way by expanding packet delivery ratio and diminishing loss of packets.

Simulation results demonstrates that the CBDDS outflanks DSR and 2ACK plans, which are picked as benchmark plans, regarding routing overhead, throughput, end to end delay and packet delivery ratio.

As future work, CBDDS approach can be utilized to address different sorts of security assaults. It can be coordinated with other message security plans to build a safe steering system for MANET's.

## 7. ACKNOWLEDGMENTS

I hereby express my sincere thanks to **Mr. Mahesh P,** Asst. Professor, Dept of CS & E, SJCE, Mysore for his continuous support in completing the above work well on time.

## 8. 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," Wireless Commun., VITAE, Chennai, India, 2011.

[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woun gang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE, Defending against collaborative attacks by malicious nodes in MANETs: A Cooperative Bait Detection Approach, January,2014, pp.65-75

[3] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, March, 2013.

[4] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: Amobile-backbone protocol for ad hoc wireless networks," in Proc. IEEEAerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[5] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. InfSecurity, vol. 7, no. 1, 2010.

[6] 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.

[7] 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.

[8] 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.

[9] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless adhoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard,"Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[11] 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.

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

[13] 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.

[14] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp.ReliableDistrib. Syst., New Delhi, India, Sep. 2009.