International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015.

ENHANCED SECURE DATA TRANSMISSION USING KEY DISTRIBUTION SCHEME SHUFFLING ALGORITHM

#1T.Karpagam·, *2Mr.S.Sivakumar

#1Research Scholar, Department of Computer Science & Applications, PGP College of Arts & Science, Namakkal, Tamil Nadu, India..
**2Asst.Professor,Department of Computer Science & Applications, PGP College of Arts & Science, Namakkal, Tamil Nadu, India..*

***Abstract*- Mobile Ad Hoc Network is an infrastructure-less, self-configuring wireless network. These unique characteristics makes it ideal for mission critical applications including Personal Area Networking (PAN), military use, Crisis-management applications such as battle field relief and remote explorations. Due to the de-centralized infrastructure, MANET becomes vulnerable to both passive and active attacks. To address such security challenges, it is very essential to detect the malicious attackers before they can accomplish any significant damages to the network. In order to detect the attackers for secure data transmission, we have proposed adaptive approach detection using key distribution scheme with shuffling algorithm. The proposed scheme eliminates the burden of certificates management and can be high level tolerance to node compromise. Our proposed work presents a more efficient solution for detecting a black hole attack with less communication cost in the MANET, which is particularly vulnerable compared to infrastructure-based networks due to its mobility and shared broadcast nature. As an adversary can successfully deploy black hole attack in the Mobile Ad hoc Networks, finally we prove that using this technique can enhance the MANET security which increases the confidentiality and integrity.**

Index Terms*- Mobile Ad Hoc Network (MANET), Key distribution scheme, shuffling algorithm, blackhole attacks, detection mechanism, malicious node and communication cost.

I. INTRODUCTION

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) [1], [2] have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming the wireless local area network [3]. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In blackhole attacks[4]. A node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called blackhole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. In grayhole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it.

Development of a security protocol in ad hoc network is not an easy task due to its unique characteristics of ad hoc wireless network, namely, shared broadcast channel, insecure operational environment, lack of central administration, lack of association between nodes, limited availability of resource and physical vulnerability [5].

In blackhole attack, a malicious node uses the routing protocol (such as AODV) to advertise itself as having the shortest path to the destination node whose packets it wants to discard/replay packets. When an attacker receives RREQ packet, then they create a reply where an extremely short route is advertised. If the malicious reply reaches to a source node before the reply from a legitimate node, a forged route has been created. Once the attacker has been able to insert itself between source and destination node, it is able to do discard/replay packets passing between them [6].

DSR [4] involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When a route to new destination needed, a source node broadcast a route request (RREQ) packet to find a route to the destination node. A valid route can discover when a RREQ reaches a destination node either itself, or an intermediate node with a fresh route to the destination node. A fresh route is a valid route entry for the destination node whose associated sequence number is greater than sequence number of RREQ packet.

When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route. DSR does not have any detection mechanism, but the source node can get all route information concerning the nodes on the route. When a link break in a route is detected, a route error (RERR) packet is used to notify other participating nodes [5]. In our approach, we make use of this feature.

In this paper, our focus is on detecting grayhole/ attacks using a dynamic source routing (DSR)-based routing technique with key distribution scheme of the shuffling algorithm. It presented that effectively detects the malicious nodes that attempt to launch grayhole/collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious 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.

II. LITERATURE SURVEY

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious 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 [5] or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories. 1) Proactive detection schemes 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 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 [6] and [5], which we considered as benchmark schemes for performance comparison purposes. In [10], Liu *et al.* proposed a 2ACK scheme for the detection of routing misbehaviour 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.

Zhou and Haas [7] first suggested using threshold cryptography to secure MANETs, with threshold signature [5], they proposed a distributed certification authority (D-CA) [6] to issue certificates to nodes, D-CA are selected from nodes in the network. Lou et al. [8] proposed a set of protocols for ubiquitous and robust access control in MANETs. They improved the model of Ref. [4] to allow every member to participate in authority decisions. Saxena et al [9] constructed several distributed access control mechanisms using certificate-based cryptography (CBC), for ad hoc groups, and investigated the applicability of various flavors of existing threshold signatures. These schemes are (t, N) -threshold (t is threshold and N is the size of network) in which every node is a D-CA. The advantage is the increased service availability since a certificate can be generated or revoked by any t nearby nodes. The disadvantage is that the compromise of any t out of N nodes would expose the certification authority's private key.

Sen et al. [10] gave a solution to detect a black hole attack in standard AODV protocol. One of the main advantages of proposed mechanism does not apply any cryptographic metrics. Instead, it protects ad hoc network by detecting and reacting to malicious activities of the intermediate nodes. Simulation results show that the technique has a significantly high detection rate with moderate network traffic hidden overhead and computation overhead. Banerjee et al. [11] proposed an approach to protecting the mobile ad-hoc network from gray hole and black hole attack. They provide a technique to discover cooperating malicious nodes, which drop a significant fraction of packets. Sharma et al. [12] tried to investigate the effects of blackhole attacks on mobile ad hoc network performance. Experimental results show network performance in the presence of a black hole is reduced up to 26%.

Raju et al. [13] present an authentication scheme for Mobile Ad Hoc Networks that is designed to combat attacks such as injecting spurious packets, tamper with packets, drop packets or impersonate another node etc. from adversaries. In the proposed scheme, every packet is authenticated at every node. Sikarwar et al. [14] give framework for secure communication in ad hoc network using dynamic key cryptography and its comparable study with intrusion detection system

A parameter acknowledgment ratio, i.e., R_{ack}, 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 Xue and Nahrstedt proposed a prevention mechanism called best-effort fault-tolerant routing (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 behaviour of the path deviates from a predefined behaviour 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.

In March 2011[13] CBDS in hybrid defense architecture is established. The protocol in present AODV, DSR nearly take account in execution. It doesn’t have the similar mechanism in finding and response. A technique to find hacker node introducing cooperative black hole attacks and black/gray hole attacks is called as cooperative bait detection scheme (CBDS). It merges the proactive and reactive architectures, and stochastically works with random adjacent node. By using the address of the neighbour node as the bait destination address and finds the malicious node by reverse tracing program and consequently prevent the attacks.

III. EXISTING SYSTEM

The existing methods the detection mechanism is of two types, they are proactive and reactive. Proactive: proactive mechanism is to find and prevent the network from the malicious node in initial stage. Reactive: reactive mechanism is to detect that node which will be active only after the destination node finds a packet drop in the packet delivery ratio. Cooperative Bait Detection Scheme is used for preventing and detecting the black hole/gray holes attacks. A black hole attack is defined as if the source node wants to send the data packets to the destination, it losses the data packets before forwarding to the destination. The gray hole is nothing but, initially the node act as the good node, after few minutes it changed into malicious node. By using the CBDS algorithm, at first the source node will select the neighbour node with the cooperation of that node. The address of the selected node is known as bait destination address to trap the malicious node to send a request reply message. By using tracing technique the adversary node is detected and prevented. If any packet drop occurs in the packet delivery ratio, an alarm is send to the source node by the destination node to activate the detection mechanism. The CBDS scheme combines the proactive scheme to find the malicious node in the initial stage and reactive mechanism to find the adversary node later in the network [14].

Limitations

The major limitation in the existing methods, packet losses is higher during the data transmission and it causes the mobility of the networks. However, link state failure is higher comparing to the AODV method. It is found that CBDS can still keep the highest throughput while avoiding interference with malicious nodes. Although their method can detect unknown attacks that raise unnatural combinations of signature-based IDS alerts, it cannot detect an unknown attack where it does not raise any alerts.

IV. PROPOSED SYSTEM

This paper proposes an enhancement of the detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching grayhole/ collaborative blackhole attacks in MANETs. In our approach, key distribution scheme with shuffling algorithm, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique.

In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. In this scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage.

In this scheme, we introduce the key distribution scheme with shuffling algorithm in the cooperative bait detection scheme. For making secure transmission, at first, we identity the black hole attackers. After that, by incorporating key distribution Center (KDC) that provide the key K value which is shared between source and the destination, it is represented in the fig.1. Source generates the key KEY, using number of hops (H_R) involved in the route and message sent time (T_S). When the KEY data is encrypted at the first level, which generates Ciphertext1

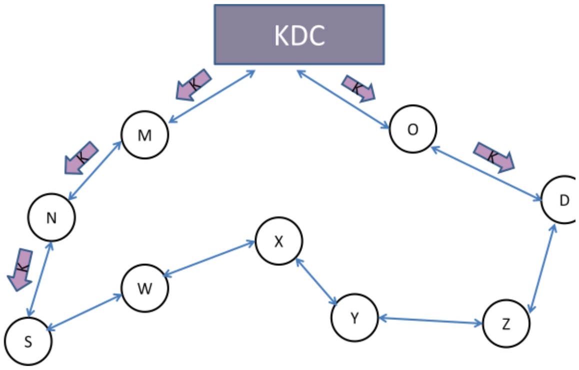


Fig.1 Key Distribution Center

In the second level, Ciphertext1,T_S and H_R are encrypted using KEY and it is presented in the fig.2. Then in the second level before encrypting the T_S and H_R , they should be shuffled using some shuffling algorithm.

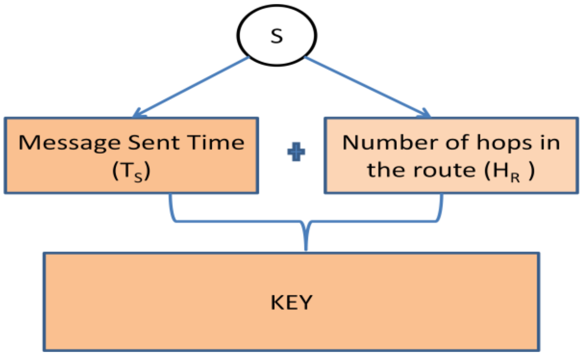
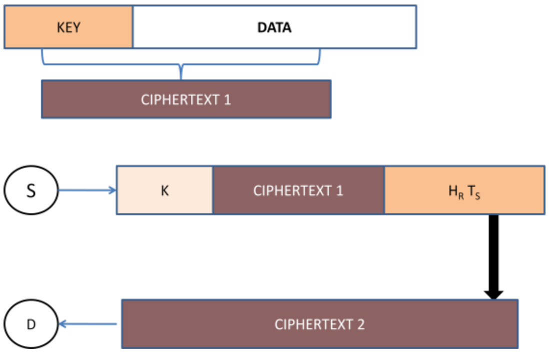

S
Message Sent Time (T_S)
+
Number of hops in the route (H_R)
KEY

Fig.2 Key Authentication

The Ciphertext2 is sent to the destination The destination makes use of K and decrypt the Ciphertext2 By making use of shuffling algorithm, destination obtains values of T_S and H_R Using T_S and $H_{R,}$ destination generates KEY Using KEY, Ciphertext1 is decrypted

To confirm that the malicious 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 X. This requires that the node had entered a promiscuous mode in order to listen to which node the last node in X sent the packets to and fed the result back to the source node. The source node would then store the node in a blackhole list and broadcast the alarm packets through the network to inform all other nodes to terminate their operation with this node. If the last node had dropped the packets instead of diverting them, the source node would store it in the blackhole list.

In this paper we propose an enhanced secure data transmission using key distribution scheme with shuffling algorithm and the proposed architecture is given in the fig.3



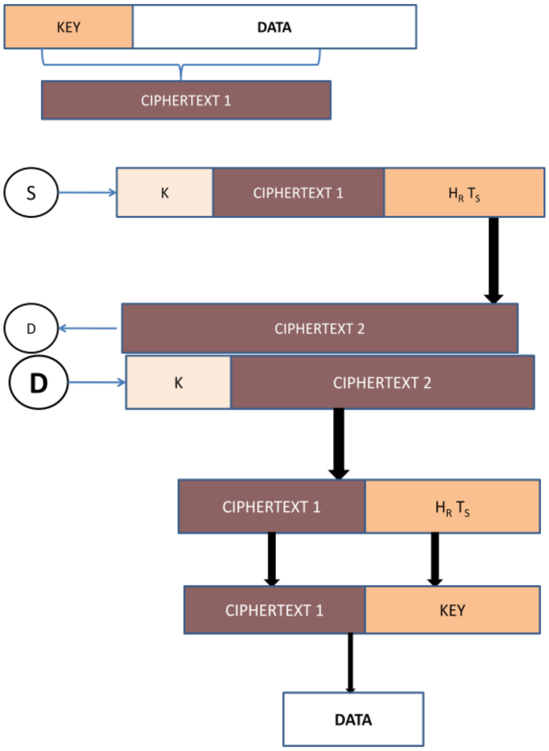


Fig .3 The proposed architecture

We have designed a key distribution scheme with shuffling algorithm (see fig 2 and fig 3) that controls the time when the packet delivery ratio falls under the same threshold. If the descending 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.

The operations of the key distribution center with CBDS are utilized in the proposed scheme. It should be noticed that the CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP. In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not. As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a grayhole attack would be detected by the CBDS the same way as those launching blackhole attacks are detected.

V. PERFORMANCE EVALUATION

A. *Simulation Parameters*

The NS2 tool [16] is used to study the performance of our CBDS with Key Distribution scheme. We employ the IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s. In our simulation, the CBDS default threshold is set to 90%. All remaining simulation parameters are captured in Table I. The network used for our simulations is depicted in Fig. 4; and we randomly select the malicious nodes to perform attacks in the network.

Performance Metrics: The metrics used to evaluate performance of proposed approach:

a)Packet Delivery Ratio (PDR): It is defined as the total number of packets received by the destination node and total number of packets originated by source node.

b)Throughput: It is defined as the total number of packets or data bits successfully delivered at the destination in a given simulation time.

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

d) 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.

First, we study the packet delivery ratio of the CBDS and for different thresholds and when the percentage of malicious nodes in the network varies from 0% to 40%. The maximum speed of nodes is set to 20m/s. Here, the threshold value is set to 85%, 95%, and the dynamic threshold, respectively. The results are captured in Fig. 6. In Fig. 6, it can be observed that DSR drastically suffers from blackhole attacks when the percentage of malicious nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing blackhole attacks.

Table I. Stimulation parameters

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	700m*700m
Simulation time	800
Malicious nodes	0%40%

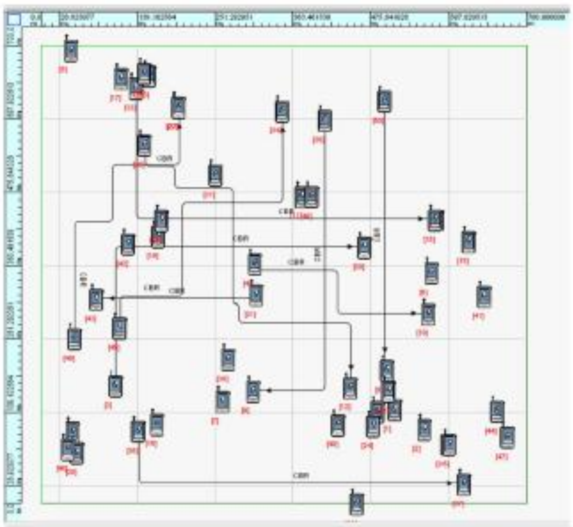


Fig.4 Network Topology

Simulation results

We used the performance metrics to validate the proposed algorithm against black hole attack and the results obtained are shown in Figure 5 and figure 6.

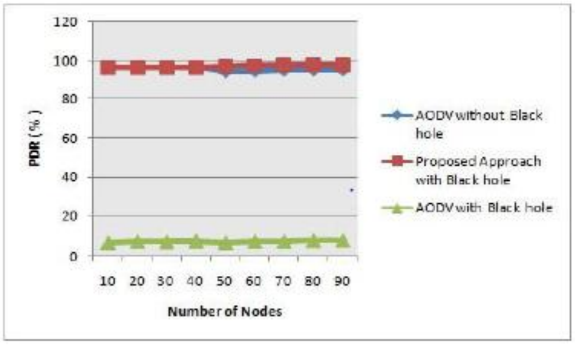


Fig.5 Packet Delivery ratio

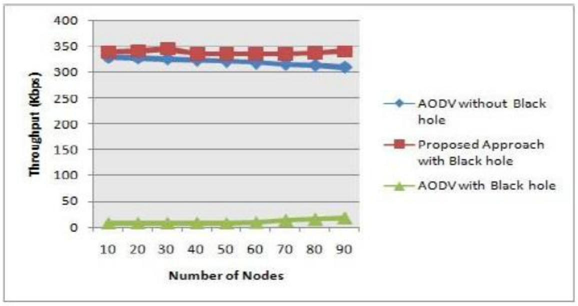


Fig. 6 Throughput

Figure 5 shows the effect to the Packet Delivery Ratio (PDR) measured for the standard AODV protocol when node mobility is varying. It is measured that Packet Delivery Ratio of standard AODV is dramatically drop by 94.1 % when there is black hole nodes in the network, but Packet delivery Ratio increases by 96.3 % when our proposed algorithm is used in the presence of black hole

Figure 6 shows the effect to PDR measured for the standard AODV protocol when numbers of nodes are varying in the network. It is measured that PDR drops by 95.2 in the presence of a black hole node in the network, but proposed algorithm increases by 97.4. Thus the proposed scheme is very significant and effective when comparing with existing methods.

VI. CONCLUSION

In this paper, we have proposed a new mechanism (called the CBDS with Key distribution scheme) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. It can be seen that Packet Delivery Ratio and Throughput of standard AODV protocol decreases due to the presence of black hole node in the network. However, the overall performance of standard AODV protocol can vary dramatically when the network conditions change. Experimental results show that the proposed algorithm achieves a very good rise in packet delivery ratio and throughput. We believe that proposed algorithm is an efficient solution for detection the black hole node in the network. As future work, we intend to 1) investigate the feasibility of adjusting our CBDS approach . To address other types of collaborative attacks on MANETs and to 2) investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

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 forMANET based on hybrid defense architecture,” in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[2] S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).

[3] C. Chang, Y.Wang, and H. Chao, “An efficientMesh-based core multicast routing protocol onMANETs,” *J. Internet Technol.*, vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” *Mobile Comput.*, 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 blackhole and cooperative blackhole 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 blackhole 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] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, 2014**.**