I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks

Aishwarya S. Anand Ukey
Dept. of Computer Science & Engineering
GGITM, Bhopal

Meenu Chawla, PhD.
Dept. of Computer Science & Engineering
MANIT, Bhopal

Virendra Pal Singh
Dept. of Computer Science & Engineering
TIT, Bhopal

ABSTRACT

Mobile Ad hoc NETwork (MANET) is considered as network without infrastructure where communication between the mobile nodes solely depends on the routing protocols which work on assumption that nodes are fully cooperative. In the presence of misbehaving nodes, most of the routing protocols show dropped performance and in some case whole of the network fails. Misbehaving nodes interrupt the data flow by either by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery or to select an alternative route if available which may again include some misbehaving nodes, thereby forming a loop, enforcing source node to conclude that data cannot be further transferred. In this paper, a new reputation based approach is proposed which deals with such misbehaving nodes and can be integrated on top of any source routing protocol Proposed approach consists of detection and isolation of misbehaving nodes and based on sending acknowledgement packets back for reception of data packets.

General Terms

Ad hoc network security, Secure Routing Protocol

Keywords

Routing Misbehavior, Non-cooperation, Misbehaving Nodes, Malicious, Acknowledgement packet transmission

1. INTRODUCTION

Mobile Ad hoc Network (MANET) [1][2][3] are self-configuring networks of mobile nodes connected by wireless links where each device is free to move independently in any direction, and will therefore changes its links to other nodes and devices frequently. Traditional routing protocols for wireless ad hoc networks assume a non-adversarial and a cooperative network setting. Basic problem with most of the routing protocols is that they trust all nodes of network and are based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly (misbehave). Most of the routing protocol designed for ad hoc network becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes.

It is also seen that most of the researches done previously, aimed on detection and prevention of external attacks. All of these researches become worthless when the malicious nodes already entered the network or legitimate nodes are compromised by attacker. Attacks performed by such malicious nodes are more dangerous as these are initiated from inside the network. Such attacks are performed by participating malicious nodes which behave well before they are compromised therefore it becomes very difficult to detect.

In this paper an acknowledgement based approach named I-2ACK is proposed, having the objective of detection and isolation of misbehaving nodes such that the network performance will not be severely degraded with the presence of misbehaving nodes.

2. SYSTEM MODEL

Security is very strong and essential service for both wired and wireless network communications. The services provided by the MANET depend on whether its security can be trusted. But characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense.

Generally routing protocol is associated with data forwarding function which in turns is concerned with forwarding data packets toward the destination through the established route. Now in order to work properly, routing protocols need trusted working environments which are not always available and in such a situation network will be vulnerable to various attacks launched by misbehaving nodes. Both routing and data-forwarding function would be affected with the presence of misbehaving nodes. Node's misbehavior can be classified [2] into following:

1) Malfunctioning: These nodes suffer from hardware failures or software errors.

2) Selfish: These nodes refuse to forward or drop data packet and can be defined into three types [3] (i.e. SN1, SN2 and SN3). SN1 nodes take participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources. SN2 nodes neither participate in the route discovery phase nor in data-forwarding phase. Instead they use their resource only for transmissions of their own packets. SN3 nodes behave properly if its energy level lies between full energy-level E and certain threshold T1. They behave like node of type SN2 if energy level lies between threshold T1 and another threshold T2 and if energy level falls below T2, they behave like node of type SN1.

3) Malicious: These nodes use their resource and aims to weaken other nodes or whole network by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control. After being selected in the requested route, they cause serious attacks either by dropping all received packets as in case of Black Hole attack [4], or

selectively dropping packets in case of Gray Hole attack [5]. For convenience such malicious nodes are referred as MN nodes.

SN2 type nodes do not pose significant threat therefore can simply be ignored by the routing protocol. On the other hand SN1, SN3 and MN nodes (defined in section II) are much more dangerous to routing protocols. These nodes interrupt the data flow by either by dropping or refusing to forward the data packets thus forcing routing protocol to restart the route-discovery or to select an alternative route if it is available which in turn may again include some malicious nodes, therefore the new route will also fail. This process form a loop which enforce source to conclude that data cannot be further transferred. This proposed work aimed on the detection and isolation of such SN1 type selfish nodes and MN type malicious nodes. SN3 type selfish nodes will be detected only when they behaves similar to SN1 type nodes.

3. RELATED WORK

Previous Approaches for Detection of Routing Misbehavior can be roughly classified [9] as:

1) Secure Routing Based Scheme: aims at securing the establishment and maintenance of routes using cryptographic (i.e. encryption and decryption) techniques.

2) Credit Based Scheme: specifically provides incentives for nodes to faithfully perform networking functions and addresses at forwarding of packets for other nodes.

3) Reputation Based Scheme: aim at reactively detecting misbehavior and proactively isolating misbehaved nodes to prevent further damage.

4) Acknowledgement Based Scheme: type of reputation based scheme; aim at reactively detecting misbehavior of nodes based on sending acknowledgement packets back for reception of data packets.

3.1 Secure Routing Based Scheme

SAODV [10] (Secure Ad hoc On Demand Distance Vector) is an extension of AODV routing protocol and is based on the assumption that each node keeps certified public keys of all nodes. All routing messages are signed and verified at each hop. SAODV uses hop count as the metric for shortest route and use hash chains to secure hop count information. SAODV provides reasonable security but still vulnerable to distance fraud attack. Also there isn’t any mechanism to detect the malicious nodes and DOS attacks.

SAR [11] (Security Aware Routing) is an extension to on demand routing protocols where each node is assigned different security level based on their trust levels. Communicate between two nodes is possible if they have equal or greater trust values. Node having a lower security level simply discards the packet. SAR only focuses on the condition where certain groups are assumed to be trustworthy thus also fails in the case of secure routing.

ARAN [12] (Authenticated Routing for Ad hoc Networks) uses a certification mechanism which is achieved through the existence of a trusted certification authority. All nodes should acquire their public key from the certification authority and before entering to network, each node applies for a certificate that is signed by the certificate server. All messages transmitted are authenticated at each hop from source to destination. Due to heavy complexity involved with the certificates, ARAN is vulnerable to various type of attack (i.e. DoS attacks). Also the load involved in the routing process forces the mobile nodes to drop the packets in order to save their resources.

3.2 Credit Based Schemes

NUGLETS: Proposed by Buttyan and Hubaux [13][14] and consists of Packet Purse Model (PPM) and Packet Trade Model (PTM). In PPM, each packet is loaded with a number of nuglets which are sufficient to reach the destination. Each intermediate node takes some nuglets from the packet for the forwarding service. In the PTM, the destination pays for the packet. Each intermediate node buys the packet from previous node for some nuglets and sells it to the next one for more nuglets until the destination buys it. This approach requires a tamper-proof hardware which is the major disadvantage of this approach.

SPRITE [15]: As opposed to nuglets scheme, SPRITE requires a central credit clearance service (CCS). While receiving a message, each node keeps a receipt and sends this receipt to the CCS to claim for payment. Major drawback includes payment to nodes by source and requires public key infrastructure.

3.3 Reputation Based Schemes

WATCHDOG AND PATHRATER [16]: Marti at al. proposed a reputation-based scheme in which two modules (i.e. watchdog and pathrater) are added on at each node. Watchdog module maintains a buffer of recently sent or forwarded data packets. Buffer is cleared only when watchdog overhears the same packet being forwarded by the next hop node over the medium and if a data packet remains in the buffer too long, the next hop neighbor is suspected to be misbehaving. Pathrater module maintains a rating for every other node, calculate a path metric and choose the best path. Major drawback is that it might not detect misbehavior in presence of ambiguous collisions, receiver collisions, false misbehavior, partial dropping etc.

CONFIDANT [17]: CONFIDENT consists of four modules: The Monitor, the Reputation System, the Path Manager, and the Trust Manager. Each node monitors the behavior of its next-hop node continuously and passes any suspicious information to the Reputation System. The Reputation System changes the rating of the suspected node and if rating of a node becomes less than certain threshold, control is passed to the Path Manager. Path Manager then controls the route cache. Trust Manager propagates warning messages in the form alarm message. The drawback of CONFIDANT includes maintenance of friends list by Trust Manager. Also there might be a situation where two nodes declare each other misbehaving through ALARM messages.

3.4 Acknowledgement Based Scheme

TWOACK [18] scheme detects misbehaving link alleviate the problem of routing misbehavior by notifying the routing protocol to avoid misbehaving nodes in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore can not be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes.

Vijaya [19] proposed another acknowledgement based scheme similar to TWOACK scheme, which detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The basic idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route. This scheme also includes multicasting method by which sender can broadcast information of misbehaving nodes so that other nodes can avoid path containing misbehaving nodes and take another path for the data transmission. Similar to TWOACK, this scheme also suffers to detect the particular misbehaving node.

Usha and Radha [20] proposed extension to the TWOACK scheme requires Nack (an end to end Ack packet) to be sent between the source and the destination. On receipt of the data packets sent by the source, destination responds with a Nack packet. If a node is found to be misbehaving in the pre calculated path, the intermediate nodes are free to divert the Nack packet through alternative paths and this path will be stored in the Nack packet along with the older path, which is extracted from the original message. On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. Possible drawback includes lot of routing overhead because of Ack and Nack packets. Also due to nodes mobility probability of Nack packet reaching to source becomes smaller with the large number of intermediate nodes between source and destination.

Zeshan [21] proposed a two-fold approach for detection and isolation of nodes that drops data packets. First approach identifies the malicious activity which is done by sending an ACK packet by each intermediate node to its source node for confirming the successful reception of data packets. If the source node does not get ACK packet by intermediate nodes then source node send again its packet for destination after a specific time. If same activity was observed again then source node broadcast a packet to declare the malicious activity in the network. Second approach identifies exactly which intermediate node is doing malicious activity. Main drawback of this scheme includes the overhead due to transmissions of acknowledgement packets by every intermediate node to the source and working of all nodes in promiscuous mode at all time.

4. I-2ACK APPROACH

4.1 Assumptions

Following assumptions are made in the proposed scheme:

1) Misbehaving nodes do not work in groups.
2) Misbehaving nodes do not send or forward false acknowledgement packet.

4.2 Logical grouping and Ack transmission

In this I-2ACK approach, all nodes of active route are logically grouped into N sets (i.e. S1, S2,….,SN) where N=n/3 (n is number of nodes on active route) such that set S1 contains first three consecutive node, set S2 contains next three consecutive nodes and so on. For convenience we refer first nodes, middle node and last node of a set as LNode, MNode, and RNode respectively. Last set SN may contain one, two or three nodes. It behaves normally if contains three nodes. If it contains two nodes then first node act as LNode and second one as RNode. If it contains single node then that node act as RNode. The sets are grouped in a total of M = N-1 groups where two consecutive sets form a group with groups G1, G2… GM such that group GM = SN-1+SN. In a set, each RNode acknowledges its LNode by sending ACK-1 packet for successful reception of data packets. In a group, RNode of second set acknowledges LNode of its first set by sending ACK-2 packet for successful reception of data packet. For example if S→N1→N2→N3→N4→N5→N6→N7→D be the active path then the nodes of active path forms three sets (i.e. S1, S2, S3) and two groups (i.e. G1, G2) shown in figure 1.

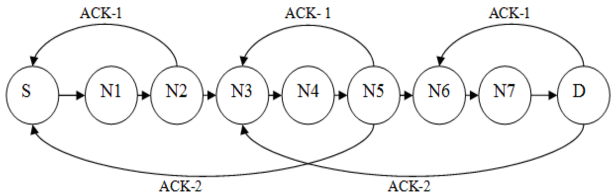

Fig. 1 Logical grouping of Nodes

4.3 Algorithm

In I-2ACK approach, each node maintains a LIST which consists of ID of every data packets sent or forwarded. After forwarding data packet to the next hop along the active route, LNode of every group will make an entry of forwarded data packet in the LIST and wait for ACK-1 and ACK-2 packet which are sent from RNode of first set and RNode of second set respectively. Also ACK-1 and ACK-2 packet must be received within time T1 and T2 respectively. From here execution of algorithm starts as follow:

```
For each group {
        For each set
        If ACK-1 is not received within T1
        Then
        LNode observe the behavior of MNode for time T3
        by rating the behavior
                And if
                Rating fall certain threshold TS
                Then
                LNode declares its MNode as misbehaving node
                Else
                LNode declares its RNode as misbehaving
                node
        Else Wait for ACK-2 for T2
        End For set
        If ACK-2 is not received within T2
        Then
        After T2 both MNode automatically GOES TO promiscuous mode and start rating the behavior of their RNodes
                And if Rating falls below threshold TS
                Then
                MNode declares its RNode as misbehaving node
                Else LNode of second set is declared as misbehaving node
        Else
        LNode deletes the ID of corresponding data packet
        from the LIST}
End For group
```

4.4 Details

Proposed approach includes following three steps:

1) Detection of malicious group: Before identifying malicious or misbehaving node, network should be aware that some malicious activity is present or not. Suppose S→N1→N2→N3→N4→N5→N6→N7→D be the active route discovered by any source routing protocol (i.e. DSR [13]). As active route is discovered, source node S will start proposed algorithm and forms N number of sets and each set consists of three consecutive nodes (i.e. LNode, MNode and RNode respectively). LNode and RNode of any set act as temporary source and temporary destination. After forwarding data packet to next hop along the active route, each LNode makes an entry of forwarded data packet in LIST and then waits for two acknowledgement packets (i.e. ACK-1, ACK-2). If any ACK-1 or ACK-2 packet is not received within their time limit T1 and T2 respectively, that group is considered as malicious group.

2) Identification of particular misbehaving node: If ACK-1 is received within time T1 then LNode waits for ACK-2 else observers its MNode by rating the behavior in promiscuous mode and if rating falls threshold TS, LNode declares its MNode as misbehaving nodes and if not, LNode declares its RNode as misbehaving nodes and then flood this information. If ACK-2 is not received within time T2, then after time T2 both MNode of that group starts rating their next hop nodes (i.e. RNode) for time T3 and when it is found that number of dropped packets exceeds threshold TS within time T3 then that RNode is declared as misbehaving node otherwise LNode of second set is declared as misbehaving node. Finally information of misbehaving node is flooded across the network.

3) Isolation and mitigation of misbehaving node: Each node of network maintains a LIST of misbehaving nodes. Thus upon receiving information of misbehaving nodes, each node update their LIST and avoid using detected misbehaving node for time T4. With the expiration of time T4, the entry of misbehaving node is temporarily deleted from the LIST thereby giving a chance to previously declared misbehaving nodes to be used by network again and if the same node is caught as misbehaving node more than certain number of time (i.e. TS1) then that node is permanently isolated from network.

In order to minimize additional routing overhead due to transmission of acknowledgement packets, a fraction of data packets will be acknowledged via a single acknowledgement packet. We refer this fraction of data packets as FRACK and by varying the FRACK, routing overhead due to transmissions of ACK-1 and ACK-2 packets can be dynamically tuned.

5. SIMULATION & RESULT ANALYSIS

Implementation of I-2ACK approach is done using ns-2 [14] by integrating it on the top of existing implementation of DSR. To show the effectiveness and efficiency of I-2ACK, a series of simulation experiments were performed. Based on these experiments, the performance of I-2ACK is compared with traditional DSR. Following section gives the details of major differences that were figured out while doing simulation experiments.

In ns-2, all simulation experiments were carried out with 100 mobile nodes moving in a 1000×1000 m. Transmission range of each mobile node is 250 m. IEEE 802.11 MAC layer was used. A random waypoint mobility model is chosen with maximum speed of 2 m/sec with pause time of 0 second. CBR transfer is used for the communication between pairs of nodes. For each CBR pairs, source and destination are chosen randomly. Each simulation lasts for 200 seconds. Experimental threshold value for misbehavior counter (allowable misbehavior per node) and time to receive acknowledgement packet (i.e. Ack-1 and Ack-2) is set to 5 and 10 respectively.

5.1 Packet Delivery Ratio

From figure 2, it is concluded that with the increase in the percent of malicious node I-2ACK shows improved packet delivery ratio as compared to DSR as DSR is not able to detect any malicious nodes so maximum time of DSR is wasted in finding the new route which may again consists of malicious nodes. In the case of I-2ACK, once malicious nodes are detected they are permanently isolated from network thus the new route is free from any malicious nodes.

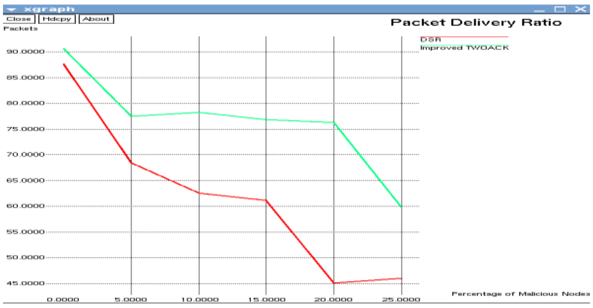

Fig. 2: Packet Delivery Ratio

5.2 Data Packet Dropped

From figure 3, it is concluded that lesser data packets were dropped in case of I-2ACK as compared to DSR. This is because malicious nodes were isolated from network once detected, so new route will not contain previously detected malicious nodes. As DSR is not able to detect any malicious nodes, more packets were dropped.

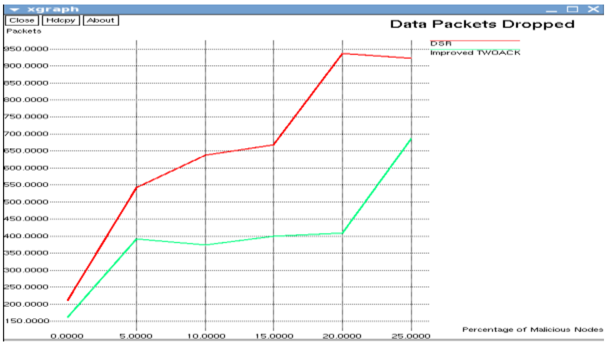

Fig. 3: Packets Dropped

5.3 Throughput

From figure 4, it is clearly seen that without any malicious node both DSR and I-2ACK have nearly same throughput. But with the increase in the percent of malicious nodes, throughput of I-2ACK is better than DSR because I-2ACK detects and isolates malicious nodes, which is not in the case of DSR. So the number of data packet received by destination is more in the case of I-2ACK.

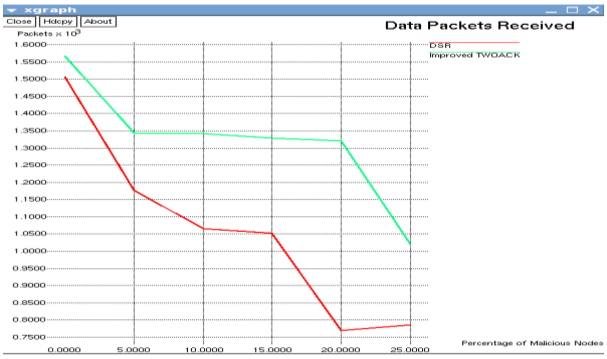

Fig. 4: Data Packets Received

5.4 Comparison with Previous Approaches

Table 1 shows the comparison of I-2ACK, with previously proposed acknowledge based schemes, based on criteria of detection of malicious link or node and number of acknowledgement packets transmitted, with the increase in number of nodes (i.e. 1,2….n) on active route.

Table 1: Comparison with other Ack based scheme

S. No	Scheme	Detects malicious link/node	Ack packets transmitted
1	TWOACK: Preventing Selfishness in Mobile Ad hoc Networks [9]	Link	n-2
2	Good Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks [10]	Link	n-2
3	Co-operative Approach to Detect Misbehaving Nodes in Manet [11]	Node	n
4	Adding Security against Packet Dropping Attack in Manet [12]	Node	n-1
5	I-2ACK	Node	~(2n/3)-1

6. CONCLUSIONS

Mobile Ad hoc network is a system of wireless mobile nodes dynamically self-organizing in arbitrary and temporary network anatomy. Misbehavior of nodes is one of a common problem in MANET as it may cause severe damage or even fails whole of the network. In this paper, investigation is done on the misbehavior of nodes and a new approach named "I-2ACK" is proposed for detection and isolation of misbehaving nodes. I-2ACK is based on sending acknowledgement packets for reception of data packets and using simple rating mechanism for counting the number of data packet such that it overcomes the problem of misbehaving nodes.

In order to show the effectiveness, I-2ACK is implemented on ns-2 and various simulations experiments were performed. Simulation results proved that I-2ACK performed better in the presence of misbehaving nodes. Also it is proved that I-2ACK has lesser routing overhead and more advantageous than previous similar acknowledgement based schemes as it requires lesser number of acknowledgement packet transmission. Future work includes inclusion of a reliable framework in mobile ad hoc network that can deals with different type of attacks simultaneously.

7. ACKNOWLEDGMENTS

Aishwarya S. Anand Ukey received Bachelor degree in Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, in 2008 and Master Degree in Technology from Maulana Azad National Institute of Technology, Bhopal, India, in 2010. He is working as Assistant professor in the Dept. of Computer Sci. & Engg. at Gyan Ganga Institute of Technology and Management, Bhopal, India. His research interest includes wireless & ad hoc networks, information security and distributed systems.

Virendra Pal Singh received Bachelor degree in Technology from Uttar Pradesh Technical University, Lucknow, India, in 2005 and Master Degree in Technology from Maulana Azad National Institute of Technology, Bhopal, India, in 2010. He is working as Assistant Professor in the dept. of Computer Sci. & Engg. at Technocrat Institute of Technology, Bhopal, India. His research interest includes ad hoc and sensor networks, information security and data warehousing.

Dr. Meenu Chawla received Master degree in Technology from Indian Institute of Technology, Kanpur, India and Doctorate degree from Maulana Azad National Institute of Technology, Bhopal, India. She is working as Associate Professor in the dept. of Computer Sci. & Engg. at Maulana Azad National Institute of Technology, Bhopal, India. Her research interest includes ad hoc and sensor network, information security, wireless network.

8. REFERENCES

[1] C. Mbarushimana, and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," in Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW '07), May 2007, pp. 679–684.

[2] Kargl, S. Schlott, A. Klenk, A. Geiss, and M. Weber, "Securing Adhoc Routing Protocols," in Proc. of the 30th EUROMICRO Conference (EUROMICRO'04), August 2004, pp. 514–519.

[3] Abdelaziz Babakhouya, Yacine Challal, and Abdelmadjid Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad Hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597.

[4] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile Ad Hoc networks," in Proc. of the 42nd annual Southeast regional conference, ACM Southeast Regional Conference, April 2004, pp. 96–97.

[5] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P. Balamuralidhar, “A mechanism for detection of gray hole attack in mobile Ad Hoc networks,” in Proc. of the 6th International Conference on Information, Communications & Signal Processing, December 2007, pp. 1-5.

[6] S. Zhong, J. Chen, and Y. Yang, “Sprite: A Simple, Cheat Proof, Credit- Based System for Mobile Ad-Hoc Networks,” in Proc. of IEEE INFOCOM’03, March 2003, pp. 1987-1997.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 2000, pp. 255-265.

[8] Sonja Buchegger Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol Cooperation of Nodes Fairness in Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), June 2002, pp. 226-236.

[9] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC’05), vol. 4, March 2005, pp. 2137-2142.

[10] K.Vijaya “Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks,” TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[11] S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp. 576-578.

[12] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," in 2008 International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[13] D.B. Johnson, D.A. Maltz, and Y. Hu, “The Dynamic Source Routing Protocol for Mobile ad-hoc Networks (DSR),” IETF Internet Draft, July 2004.

[14] “The Network Simulator - ns-2,” isi.edu, [Online] Available: http://www.isi.edu/nsnam/ns/ [Accessed: Jan, 2013].