A Timer Based Acknowledgement Scheme for Node Misbehavior Detection and Isolation in MANET

Ramasamy Murugan[1] and Arumugam Shanmugam[2]
(Corresponding author: Ramasamy Murugan)

Department of Computer Applications & Bannari Amman Institute of Technology[1]
Sathyamangalam, Tamil Nadu, India - 638401
Department of Electronics and Communication Engineering & Bannari Amman Institute of Technology[2]
Sathyamangalam, Tamil Nadu, India - 638401
(Email: muruganraam75@yahoo.com)
(Received Apr. 19, 2011; revised and accepted July 13, 2011)

Abstract

The nodes in the network that causes dysfunction in network and damage to the other node are misbehaving nodes. They support the flow of route discovery traffic but interrupt the data flow causing the routing protocol to restart the route discovery process. In this paper, an efficient timer based acknowledgement technique is proposed to detect and isolate the misbehaving nodes and can even find a possible alternate route in case when the number of misbehaving nodes is greater than minimum count. This involves a detection timer and forward counter that help to reduce the number of acknowledgements thus reducing the delay and overhead. This approach is keenly focusing on acknowledgement of nodes regarding the misbehaviors so that the source takes the corresponding action. Simulation results show that the timer based acknowledgement scheme attains good packet delivery ratio with reduced packet drop, delay and overhead, when compared with secured on-demand routing protocol.

Keywords: Forward counter. misbehaving nodes, mobile ad hoc networks, timer based acknowledgement

1 Introduction

A mobile ad hoc network (MANET) is a collection of dynamic, independent, wireless devices that groups a communications network, devoid of any backing of a permanent infrastructure. The eventual goal of designing a MANET network is to make available a self-protecting, "dynamic, self-forming, and self-healing network" for the dynamic and non-predictive topological network [9]. According to the positions and transmission range, every node in MANET acts as a router and tends to move arbitrary and dynamically connected to form network. The topology of the ad hoc network is mainly interdependent on two factors; the transmission power of the nodes and the Mobile Node location, which are never fixed along the time period [15].

Ad hoc networks excel from the traditional networks in many factors like; easy and swift installation and trouble-free reconfiguration, which transform them into circumstances, where deployment of a network infrastructure is too expensive or too susceptible [3]. MANETs have applicability in several areas like in military applications where cadets relaying important data of situational awareness on the battleground, in corporate houses where employees or associates sharing information inside the company premises or in a meeting hall; attendees using wireless gadgets participating in an interactive conference, critical mission programmer for relief matters in any disaster events like large scale mishaps like war or terrorist attacks, natural disasters and all. They are also been used up in private area and home networking, "location-based" services, sensor networks and many more adds up as services based on MANET [18]. The three major drawback related to the quality of service in MANET are bandwidth limitations, vibrant and non-predictive topology and the limited processing and minimum storage of mobile nodes [17].

The wireless nature and inherent features of mobile ad hoc networks make them vulnerable to a wide variety of attacks. The attacks on MANETs can be classified into various criteria as discussed in [11, 13, 16, 18].

In MANETs, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets.

Routing protocols basically performs two important functions: Routing function and Data-Forwarding function. Routing function performs route discovery and route maintenance activity. Data-Forwarding function is concerned with forwarding data packets toward the destination through the established route. To perform these functions, the 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, 15] as malfunctioning, selfish or malicious nodes. Malfunctioning nodes suffer from hardware failures or software errors. Selfish nodes refuse to forward or drop data packet. It can take participation in the route discovery and route maintenance phases but refuses to forward data packets to save its resources. Malicious 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.

In this paper, an efficient timer based acknowledgement technique is proposed to detect and isolate the misbehaving nodes and can even find a possible alternate route in case when the number of misbehaving nodes is greater than minimum count. This involves a detection timer and forward counter that help to reduce the number of acknowledgements thus reducing the delay and overhead. This approach is keenly focusing on acknowledgement of nodes regarding the misbehaviors so that the source takes the corresponding action. Simulation results show that the timer based acknowledgement scheme attains good packet delivery ratio with reduced packet drop, delay and overhead, when compared with secured on-demand routing protocol.

1.1 Previous Work and Proposed Work

In our previous work [7], we have developed a combined solution for routing and MAC layer attacks. Our approach, made use of three techniques simultaneously which consists of a cumulative frequency based detection technique for detecting MAC layers attacks, data forwarding behavior based detection technique for detecting packet drops and MAC based authentication technique for packet modification. Our combined solution presented a reputation value for detecting the malicious nodes and isolated them from further network participation till its revocation.

In paper [1], a new reputation based approach is proposed that deals with routing misbehavior and consists of detection and isolation of misbehaving nodes. Here, data forwarding function is concerned with forwarding each data packet towards the destination through the established route. For a group, it is assumed that there are two sets. The source node of the first set must be acknowledged by the destination node after the successful reception of the data packets. Also, the destination node of the second set must send the second acknowledgement to the source node of the first set after the successful reception.

This has certain drawbacks as Sending of acknowledgement packets and counting the number of data packets individually is time consuming and even causes overhead. The process is always accompanied with delay.

In this paper, in order to overcome these drawbacks, we propose the following approach. For every group of nodes, a detection timer with the specific time interval is assigned. Once the source starts forwarding the packets, the timer starts. A forward counter is maintained so that it will be updated during the packet entering and leaving the node. When the detection timer expires, the destination node is checked for those data packets which have entered and left the node. If the forward count is below a predefined threshold, negative acknowledgement (NACK) is sent to the source node of first set. Otherwise the positive acknowledgement (PACK) is sent. This process is repeated for each group of nodes.

The advantage in our approach is that there is no need of sending acknowledgement for reception of each data packet since it is processed in group-wise and it minimizes the waiting period for acknowledgement and also overhead is reduced.

2 Related Works

Mamatha et al. [5] investigated the performance degradation caused by such malicious nodes (misbehaving) in MANETS. They have proposed and evaluated a technique called, (AODV+ACK+PFC) to detect and mitigate the effect of such routing misbehavior. In future the enhancement may be done by evaluating for more number of nodes and network parameters. Further the scheme may also be extended for identifying and preventing more number of network layer attacks; so that the approach can be made more robust against attacks.

Rajaram et al. [12] proposed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, they have designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the Cipher Block Chaining (CBC-X) mode of authentication and encryption.

Anandukey et al. [1] investigated the misbehavior of nodes and a new approach is proposed for detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol such as DSR and is based on sending acknowledgement packets for reception of data packets and using promiscuous mode for counting the number of data packet such that it overcomes the problem of misbehaving nodes. Also proposed approach has lesser routing overhead and more advantageous because it requires lesser number of acknowledgement packet transmission. In future, they will include some authentication mechanism to make sure that

the ACK packets are genuine and also including mechanism to punish misbehaving nodes.

Liu et al. [4] proposed a hardware based two-timer scheme to detect the misbehaving nodes. The features of the proposed scheme include high detection of misbehaving nodes, low false positive, minor changes to software layer, and simple to implement in hardware. There are only two timers and a counter needed. Thus this scheme can be implemented at very low cost.

Manvi et al. [6] investigated the performance degradation caused by such selfish (misbehaving) nodes in MANETs. They have analyzed and evaluated a technique, termed 2ACK, to detect and mitigate the effect of such routing misbehaviour. They have embedded some security aspects with 2ACK to check confidentiality of the message by verifying the original hash code with hash code generated at the destination. One advantage of the 2ACK scheme is its flexibility to control overhead.

Pirzada et al. [10] presented a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network, without engaging any cryptographic means. With the help of extensive simulations, we demonstrate that our scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.

Ren et al. [14] proposed a defense scheme that includes both the detection and response mechanisms. The detection signals include the frequency of receiving RTS/CTS packets, frequency of sensing a busy channel (signal interference), and number of RTS/DATA retransmissions. The response scheme is based on the ECN marking mechanism. Through extensive ns2 network simulations, we demonstrate the existence of high good put and delay jitters under the pulsing attack mode.

Misbehaving nodes do not forward data packets and also they do not drop acknowledgement packets. False acknowledgement packets are never sent or forwarded by misbehaving nodes.

3. Timer Based Acknowledgement Scheme

In the proposed scheme, it is assumed that, each node maintains a LIST which contains ID of every data packets sent or forwarded.

3.1 Grouping of Nodes and Transmission of Acknowledgement Packets

As soon as the desired route is found, all the nodes of the desired route are logically grouped into N sets (i.e. M_1, M_2, $M_3 \ldots M_n$), where M=m/3 (m is the number of nodes in the desired route) such that the group M_1 contains first three consecutive nodes and group M_2 contains next three consecutive nodes (as in Figure 1) and so on. Hence a group M_1 consists of the source S which is First node referred as FNode and the intermediate node referred as INode and the Last node of the group is referred as LNode. For example if $S \rightarrow R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6 \rightarrow R_7 \rightarrow D$ is the desired route then nodes of the desired path forms three groups(i.e M_1, M_2, M_3).

The Group $M_1 = S \rightarrow R_1 \rightarrow R_2$
Group $M_2 = R_3 \rightarrow R_4 \rightarrow R_5$
Group $M_3 = R_6 \rightarrow R_7 \rightarrow D$

The proposed work focuses on detecting selfish nodes which drop packets such that the other nodes can never use it. Here the selfish behavior of the nodes is considered as misbehaving because they drop packets to save battery power. In order to track the incoming packets and outgoing packets a forward counter F_c is used in each node. The forward counter is updated when a packet leaves the node and when a packet enters the node. A detection timer Dtimer is assigned for every group of nodes with specific time interval. When the Dtimer starts the source node, i.e FNode starts forwarding the packets and when the Dtimer expires, the last node say LNode send as acknowledgement to the SNode.

The proposed scheme aims to detect and isolate the misbehaving nodes.

3.2 Detecting Misbehaving Nodes

The nodes start forwarding the packet upon request. When this action begins, the D timer starts. The forward counter is on and this gets incremented or decremented according to the flow.

When the packet enters the node, the F_c is incremented and when the packet leaves node F_c is incremented.After the Dtimer expires, the last hop node of the group compares the value of F_c with forward counter threshold F_{ct}. If F_c of LNode is equal to F_{ct} then PACK is sent else NACK is sent. In this manner the process continues for every group of nodes.

The merit of this approach is that there is no need of sending acknowledgement for reception of each data packet since it is processed in group-wise and it minimizes the waiting period for acknowledgement and also overhead is reduced.

3.3 Mitigating Misbehaving Nodes

If the source is informed with PACK, the route is considered as normal. If NACK is informed to the source node, then the source node of every group counts the NACK of each node. If $NACK_c$ is greater than $NACK_{cmax}$, then the node is considered as misbehaving and this information is broadcasted to all other groups in the route.

From the broadcast information, the destination node checks the number of misbehaving nodes along the route and this information is sent as a feedback to the source node. If the source node finds that only limited number of misbehaving nodes (say 2) in the route, then that particular

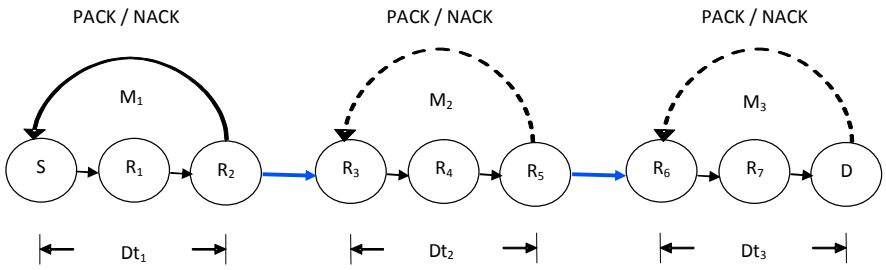

Figure 1: Grouping of nodes and transmission of PACK / NACK

Algorithm 1: Detecting Misbehaving Nodes

```
1 Begin
2 For each group, As the Dtimer starts, the SNode starts
  forwarding the packets
3  If a packet enters the node then
4    Fc=Fc+1
5  Else if a packet leaves the node then
6    Fc=Fc-1
7  Endif
8   If the Dtimer expires then
9     If FC(LNode)==Fct then
10      PACK is sent to SNode
11    Else
12      NACK is sent to SNode
13    Endif
14  Endif
1 5 Endfor
16 End
```

nodes are marked as rejected and bypass route is established excluding those nodes.

When the number of misbehaving nodes exceeds the minimum count, then the entire route is treated as misbehaving and an alternate route is established for the transmission, by the source.

Algorithm 2: Mitigating Misbehaving Nodes

```
1 Begin
2 For each group, Each source node SNode counts ACK
  received from LNode for the time T1
3   If NACKC > NACKCmax then
4       Source node SNode broadcast the information of
        misbehaving nodes to all groups
5       If no. of misbehaving nodes > Limited no. of
          misbehaving nodes then
6             Alternate route is chosen
7       Else
8             Misbehaving nodes are bypassed
9       Endif
9    Else
10      Route is considered to be normal
11    Endif
     12  Endfor
13 End
```

4 Performance Analysis

4.1 Simulation Model and Parameters

We use Network Simulator (NS2) [8] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in Table 1

Table 1: Simulation Settings

no. of Nodes	25,50,…125
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
Misbehaving Nodes	5,10,15,20,25

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

The simulation results are presented in the next section. We compare our Timer based Acknowledgment (TimeACK) scheme in presence of malicious node environment.

4.3 Results

Case 1:

In our first experiment, we have taken a scenario for a given source and destination pair (25, 89). We gradually increase the number of misbehaving nodes along the established path for this pair.
Depending upon the source, destination pair and the desired path between them, the number of misbehaving nodes may vary. Based on the number of misbehaving nodes, say 2 (minimum count), the source node determines whether to take an alternate path or reroutes the entire traffic through that path.

Figure 2 shows the average end-to-end delay for the increasing misbehaving nodes. In the proposed scheme TimerACK, as the nodes form groups, the number of acknowledgement packets that are exchanged are relatively less compared to the without proposed scheme where the nodes does not form groups and hence each node have to send acknowledgement to its previous node. Hence the delay is higher for without proposed scheme.

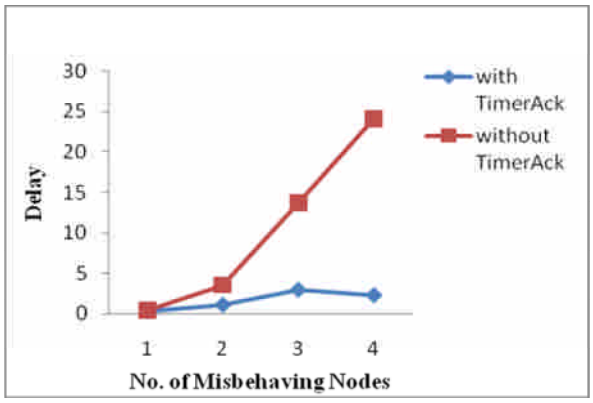

Figure 2: no. of misbehaving nodes vs. delay

Figure 3 shows that the delivery ratio of the proposed scheme is steady even though the number of attackers increases. This is because, the TimerAck scheme uses a Dtimer which detects the misbehaving nodes within a particular time T in which the number of misbehaving nodes greater than 2, an alternate path is chosen. Where as in the without proposed scheme the delivery ratio decreases when the misbehaving node increases above 2.

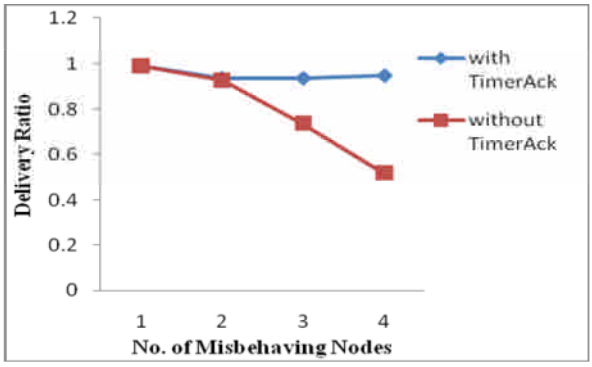

Figure 3: no. of misbehaving nodes vs. delivery ratio

Figure 4 shows that the proposed scheme TimerAck, the packet drop is minimum compared to the without proposed scheme. Initially when the number of attackers is one, the number of packets dropped is 35 and as the attackers increases say 4, the packet drop also increases gradually to 460 packets ie., approximately 13 times of the initial drop. Whereas in case of without proposed scheme the initial drop is 47 packets and as the number of attackers increases, the packet drop also increases suddenly to 5000 packets i.e. approximately 100 times of the initial drop.

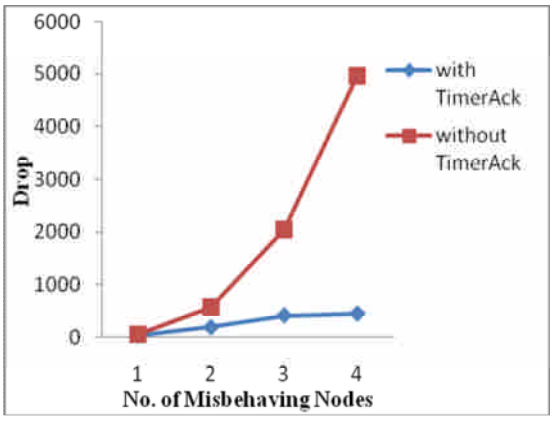

Figure 4: no. of misbehaving nodes vs. drop

From Figure 5, it is clear that the overhead increases as the number of misbehaving nodes increases. Even though the number of acknowledgement exchanges is less, the overhead for the proposed increases gradually because as the number of attackers increases, the source node chooses an alternative path.

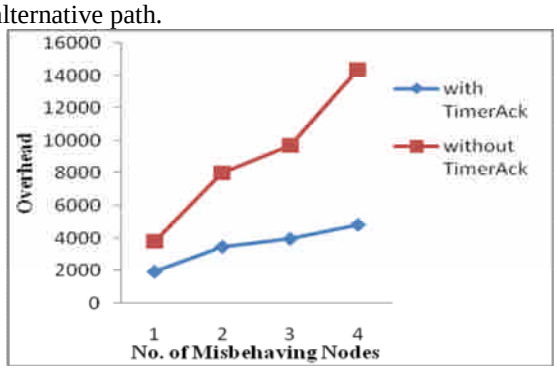

Figure 5: no. of Misbehaving Nodes Vs Overhead

Case 2:

In our second experiment, we have taken another scenario for a given source and destination pair (13, 99). We gradually increase the number of misbehaving nodes along the established path for this pair.

The results of Case 2 are similar to Case 1 where a different source and destination pair are chosen. As in case1, the delay, the delivery ratio, packet drop and the control overhead are analyzed for Case 2 and it is shown in Figures 6, 7, 8 and 9 respectively. In the results it is clear that the proposed scheme TimerAck has lower delay, higher delivery ratio, less packet drop and lower control overhead compared to without proposed scheme.

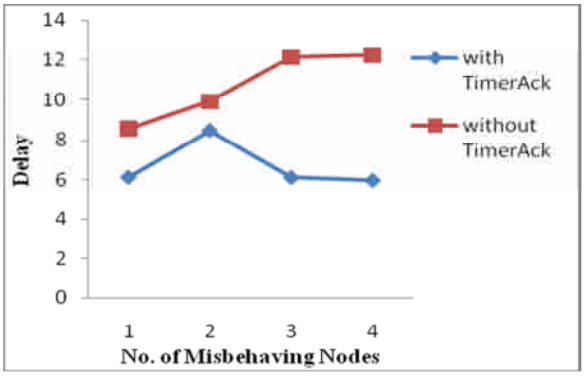

Figure 6: no. of misbehaving nodes vs. delay

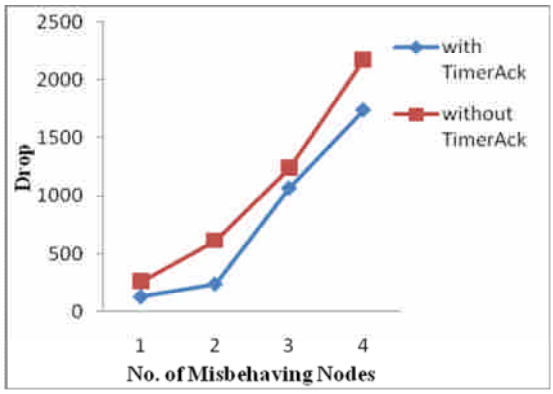

Figure 8: no. of misbehaving nodes vs. drop

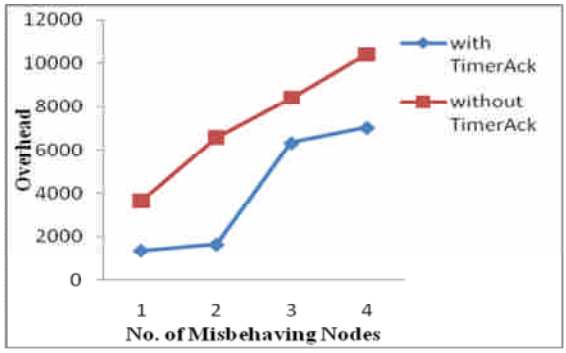

Figure 9: no. of misbehaving nodes vs. overhead

5 Conclusion

In this paper, we propose an efficient timer based acknowledgement scheme that detects and isolates the misbehavior nodes in MANET. When a node starts to forward the packet, a detection timer (Dtimer) starts and a forward counter (Fc) is used to update the packets entering and leaving the node. After Dtimer expires, the last hop node of the group verifies the value of Fc. When Fc is below the predefined threshold, source node is informed with the negative acknowledgement (NACK) otherwise with positive acknowledgement. For PACK, the route is normal else the source node counts the NACK of each node. If NACK count exceeds maximum NACK count, then the node is assigned as misbehaving and this information is broadcasted to all other groups.

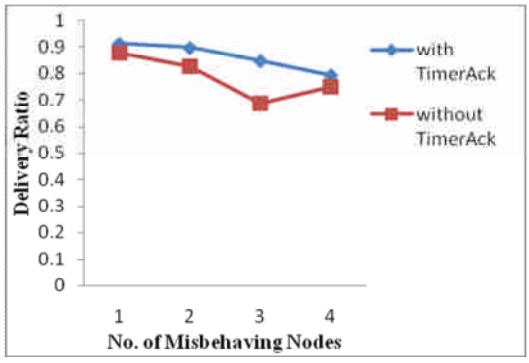

Figure 7: no. of misbehaving nodes vs. delivery ratio

If the source node as per the information of destination node finds that only limited number of misbehaving nodes (say 2) in the route, then that particular nodes are marked as rejected and bypass route is established excluding those nodes. When the number of misbehaving nodes exceeds the minimum count, then the entire route is treated as misbehaving and an alternate route is established for the transmission. This process is efficient technique for route discovery since the delay and overhead is reduced. By simulation results, we have shown that the timer based acknowledgement scheme attains good packet delivery ratio with reduced packet drop, delay and overhead, when compared with existing acknowledgement based scheme.

References

[1] A. S. Anandukey and M. Chawla, "Detection of packet dropping attack using improved acknowledgement based scheme in MANET," *International Journal of Computer Science Issues I*, vol. 7, no. 1, pp. 12-17, 2010.

[2] S. Dhanalakshmi and M. Rajaram, "A reliable and secure framework for detection and isolation of malicious nodes in MANET," *International Journal of Computer Science and Network Security*, vol..8, no.10, pp. 184-190, 2008.

[3] Y. Huang, B. Jin, J. Cao, G. Sun, and Y. Feng, "A selective push algorithm for cooperative cache

consistency maintenance over MANETs," *EUC*, pp. 650-660, 2007.

[4] H. Liu, J. G. Delgado-Frias, and S. Medidi, "Using a two-timer scheme to detect selfish nodes in adhoc networks," in *6th IASTED International Conference Communication, Internet and Information Technology*, pp.179-184, Alberta, Canada, 2007.

[5] G. S. Mamatha and S. C. Sharma, "A new combination approach to secure manets against attacks," *International Journal of Wireless & Mobile Networks*, vol.2, no.4, pp. 71-80, 2010.

[6] S. S. Manvia, L. B. Bhajantrib, and V. K. Vagga, "Routing misbehavior detection in manets using 2ACK," *Journal of Telecommunication and Information Technology*, vol 4, no. 1, pp. 105-111, 2010.

[7] R. Murugan and A. Shanmugam, "A combined solution for routing and medium access control layer attacks in mobile ad hoc networks," *Journal of Computer Science*, vol. 6, no. 12, pp.1416-1423, 2010.

[8] Network Simulator. http://www.isi.edu/nsnam/ns

[9] M. E. Orwat, T. E. Levin, and C. E. Irvine, "An ontological approach to secure MANET management," in *Proceedings of the Third International Conference on Availability, Reliability and Security*, pp. 787-794, 2008.

[10] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad hoc wireless networks," *International Journal of Network Security*, vol. 3, no. 2, pp. 191-202, 2006.

[11] M. K. Rafsanjani, A. Movaghar, and F. Koroupi, "Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes," *World Academy of Science, Engineering and Technology*, vol.2, pp. 351-355, 2008.

[12] A. Rajaram and S. Palaniswami, "Malicious node detection system for mobile ad hoc networks," *International Journal of Computer Science and Information Technologies*, vol. 1, no. 2, pp. 77-85, 2010.

[13] S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against mobile ad hoc networks routing protocols," in *5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting*, pp. 147-152, Liverpool, UK, 2004.

[14] W. Ren, Dit-Yan Yeung, Hai Jin and Mei Yang, "Pulsing RoQ DDoS attack and defense scheme in mobile ad hoc networks," *International Journal of Network Security*, vol. 4, no. 2, pp. 227-234, 2007.

[15] M. I. M. Saad and Z. A. Zukarnain, "Performance analysis of random-based mobility models in MANET routing protocol," *European Journal of Scientific Research*, vol. 32, no. 4, pp. 444-454, 2009.

[16] N. Shanthi, L. Ganeshan and K. Ramar, "Study of different attacks on multicast mobile adhoc network," *Journal of Theoretical and Applied Information Technology*, vol. 9. no. 2, pp. 45-51, 2009.

[17] M. Uma and G. Padmavathi, "A comparative study and performance evaluation of reactive quality of service routing protocols in mobile adhoc networks," *Journal of Theoretical and Applied Information Technology*, vol. 6, no. 2, pp. 223-229, 2009.

[18] Y. Xiao, X. Shen, and D. Z. Du, *Wireless Network Security*, Springer, 2006.

R. Murugan received his M.C.A. degree in Computer Applications from the Bharathiar University and M.E. degree in Computer Science and Engineering from the Anna University in 1998 and 2005 respectively. Now he is pursuing Ph.D. degree in Anna University. Currently, he is an Associate Professor in the Department of Computer Applications at Bannari Amman Institute of Technology, INDIA. He has published about 12 refereed journal and conference papers. His research interest covers Mobile Computing and Ad Hoc Networks Security.

A. Shanmugam received the B.E Degree from PSG College of Tech Coimbatore and ME Degree from College of Engineering, Guindy, Chennai in 1978 and Ph. D. in Electrical Engineering from Bharathiyar University in 1994. He was the Professor and Head of Electronics and Communication Engineering Department at PSG College of Technology, Coimbatore during 1999 to 2004. Authored a book titled "Computer Communication Networks" which is published by ISTE, New Delhi, 2000. He is currently the Professor and Principal, Bannari Amman Institute of Technology, Sathyamangalam. He is in the editorial board of International Journal Artificial Intelligence in Engineering & Technology (ICAIET), University of Malaysia, International Journal on "Systemics, Cybernetics and Informatics (IJSCI)" Pentagram Research Centre, Hyderabad, India.