Indian Journal of Science and Technology, Vol 8(14), DOI: 10.17485/ijst/2015/v8i14/70696, July 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Hash based Technique to Identify the Selfish Node in Mobile Ad-hoc Network

G. Vennila* and D. Arivazhagan

Department of Information Technology, AMET University, Chennai - 603112, India; g.vennila265@gmail.com, arivazhagand@hotmail.com

Abstract

Mobile Ad-hoc NETwork (MANET) is a collection of mobile nodes that communicate with other node without any defined network. The node which decline to share its resource with other nodes is a selfish node. The main idea of selfish node is to drop the data packets and preserve the resource for its own use. The co-operation between the nodes is not guaranteed when the node behaves as selfish nodes. Most of the existing techniques use cryptographic algorithm such as Message Authentication Code (MAC), Rivest Shamir Adelman (RSA) etc, in identifying the selfish node. All of those techniques are take more time to find out the selfish node behavior. This paper applies hash function to identify the misbehaving node. The Hash function is a technique used in the Route Reply (RREP) to authenticate the message, which works in an efficient way. The result shows the better performance in terms of packet delivery ratio up to 70% and time delay has been reduced up to 80% compared to the existing Dynamic Source Routing (DSR) protocol.

Keywords: Hash Function, Mobile Ad-Hoc Network, RREP, RREQ, Selfish Node

1. Introduction

Mobile Ad hoc Networks (MANET) is one of ubiquitous areas in the field of research in wireless network at present. MANET is a collection of mobile devices that communicate with one another without any pre-defined network. The Ad-hoc network allows the mobile devices to join as well as to leave from the network at any point of time[6]. Each mobile device in Mobile Ad-hoc Network can perform as router and as a host to share the resources to other device willingly[2]. However, some of the nodes decline to share its resource to other node that specific node is act as a selfish node or misbehavior node. This mechanism is implemented under Dynamic Source Routing (DSR) protocol. The DSR protocol is an on-demand routing protocol, which has two important phases: Route Discovery and Route Maintenance, which works mutually to permit the nodes to determine and maintain routes to destination. The DSR protocol is collaborated by one of the network layer attack called Selfish node attack[1]. The node accepts the RREQ (Route Request), and it forwards the request until it reaches the destination. Any node in between the sender and the receiver can act as a misbehave node, which refuse to share its resources to other node. This paper has proposed a novel algorithm based on hash function to identify the selfish node in DSR protocol in MANET. In section 2 describes the DSR Protocol and effect of node misbehavior. The related works are discussed in section 3. The proposed algorithm is explained in section 4. The performance analysis is presented in section 5. Finally, the conclusion is presented in section 6.

2. DSR Protocol and Effects of Selfish Node

The DSR protocol is a routing protocol in mobile ad-hoc network. It establishes the route across multiple nodes

*Author for correspondence

in network based on the user request. This protocol consists of two main phases: Route Discovery and Route Maintenance, which allows the mobile node to find and maintain the path from source to destination.

2.1 Route Discovery

The route discovery phase broadcast the Route REQest (RREQ) to find the best path from source to destination[7]. The RREQ consists of source address, destination address, sequence number and hop count. The Source Node (SN) wants to communicate with the Destination Node (DN). Consequently; it initiates the route discovery process by sending the RREQ message. Once the neighbor node receive the RREQ from the source, it checks the route cache whether it has a path to reach destination. If the route cache has a path, it sends the Route REPly (RREP) that contains path information. Else, it forwards the RREQ to next neighbors until the request reach destination. If the node is destination, it sends the Route Reply to source through the message RREP, which contains route information.

The Source Node (SN) wishes to send the packet to Destination Node (DN). Therefore, the node SN sends RREQ to its neighbor node B. The Route Request contains address of source, destination, sequence number and hop count. Upon receiving the request from source, the node B checks the possible path in its route cache. If the possible path exists in route cache, it immediately sends the Reply via RREP message. Otherwise, the node B rebroadcast RREQ to next neighbor node C. If the node C is not Destination and path is not available in route cache, it forwards the RREQ to next node DN. If the node DN is Destination Node, it sends to the next node C[3]. Subsequently, the Node C sends same reply to the next Node B. If the Node B is not a source, it forwards the reply to the next Node SN. The SN receives the reply that contains path in reverse order (DN – C – B – SN). Consequently, the Source Node starts to send the packet to Destination Node. This route discovery process is depicted in Figure 1.

2.2 Route Maintenance

The route maintenance is an important phase to manage the link breaks between sender and receiver by the message Route Error (RERR).The Source Node validates for the successful packet transmission to the destination through the message Acknowledgement (ACK)[8].

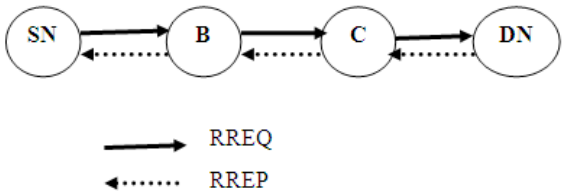

Figure 1. Route Discovery Process.

2.3 Effects of Selfish Node

The node misbehavior can be any node in network which collects the packet from the source and drops it for future use. This kind of behavior is known as "Selfish Node". When the SN wants to send packet to the DN, it initiates the Route Discovery process as shown in Figure 1. The SN sends RREQ to its nearest neighbor node. The node B and SFN is nearest node of Source. Therefore, it sends the request to node B and also SFN. The node B is not a destination and it does not have path in its route cache to reach destination. However, the node B forwards the RREQ to its adjacent node until reach Destination. The node SFN receives the request from Source and it immediately sends RREP to the SN. Upon receiving the Reply from SFN, the Source sends packet to SFN. Hence, the node SFN collects the packet in this way and drops it. Even if the node DN sends the Reply to SN, the SN already sends the packets to SFN. Therefore, it ignores the Destination Node reply. This behavior of selfish node is illustrated in Figure 2.

3. Related Works

A lot of methods have been proposed to detect selfish nodes in mobile ad hoc network. All of these methods can be categorized as Credit based method, Reputation based method and Acknowledgement based method[4].

3.1 Credit based Method

The credit based technique is to give incentive for nodes which truly perform networking functions. The payment

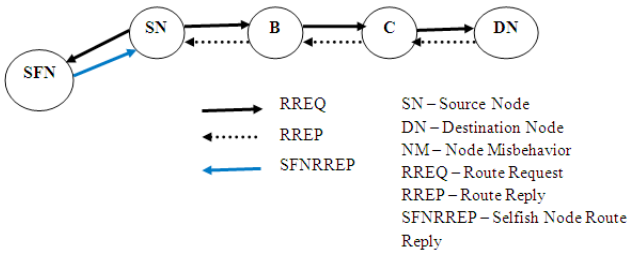

Figure 2. Behavior of Selfish Node.

system may be set up to achieve this particular goal. The Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. Credit based schemes can be applied using two models:

1) The Packet Purse Model (PPM) and 2) The Packet Trade Model (PTM)[5].

3.2 Reputation based Methods

The Reputation based techniques build a reputation metric for each node according to its behavioral pattern. A monitoring method used by most schemes in this type is called a watchdog. Watchdog was the first proposed method by Marti et al.[13] to detect the misbehaving node. This kind of scheme use two models are watchdog and pathrater model. The watchdog model was implemented in DSR protocol. It is based on neighbor monitoring scheme to identify the selfish node. Pathrater defines a route without including selfish nodes or misbehaving nodes lying on the paths. This mechanism is rewarded for selfish nodes. The difficulty in watchdog model is not detect a misbehaving node in the presence of 1) Ambiguous collisions 2) Receiver collisions 3) Limited transmission power 4) False misbehavior 5) Partial dropping[10–12] use similar monitoring schemes but it propagates collected information to its nearby nodes and are vulnerable to false praise and false accusation attacks.

3.3 Acknowledgement based Methods

The Acknowledgment based methods rely on the reception of an acknowledgment to verify that a packet coming from destination. Liu et al.[9] proposed 2ACK system where the nodes openly send acknowledgment to detect the node misbehavior. The major disadvantage in this 2ACK is that the acknowledgements overhead is increased and to reduce the same kind of problem, the improved 2ACK has been proposed by P. Samba Siva Rao et al[1], which depends on 2ACK and reduces the number of acknowledgments.

4. Proposed Work

The proposed work uses an algorithm based on cryptographic hash function to identify the node misbehavior. The hash function is a technique by which the message is authenticated that proves a message is successfully coming from the source. The algorithm has the following phases: Initialization phase, Hash generation at Destination, Hash generation at Source, Node Misbehavior Identification and Packet Forwarding phase.

4.1 Initialization Phase

The initialization phase initiates RREQ which consists of Source address, Destination address, Sequence number, Hop count. In this phase, it broadcast RREQ to all the neighbor nodes of Originator in order to find the path from source to destination; initially it sends RREQ to next node. If it is destination then it sends RREP that contains route information. Otherwise, it adds its own address in RREQ and forwards the RREQ till it reach destination.

The sender node sends RREQ to its adjacent nodes such as (Neighbor node-A, Neighbor node-B and Selfish node-SFN). If the Selfish Node (SFN) accepts RREQ from Sender Node, it will not forward the request to next adjacent node. However, If the adjacent (neighbor) node-A accepts RREQ from Sender and not a destination, it rebroadcast RREQ to next node (Neighbor Node-B). If the neighbor node-B is also not a destination, it forwards the RREQ to next neighbor node (Destination). Finally, the Destination node receives RREQ from sender node. This phase is depicted in Figure 3.

4.2 Hash Generation at Destination

The hash code is generated by using the efficient technique called hash function. The hash code is calculated by using the following formula,

$$HC = H_K (M) \quad (1)$$

The product of original Message (M) and Hash function (H) with secret key produce the output called as Hash Code (HC). Once receives the RREQ from source; the Destination Node generates hash code by using the above formula. Subsequently, the hash code is appended

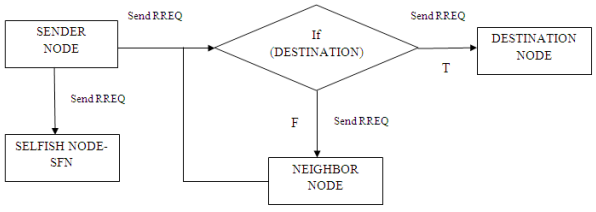

Figure 3. Initialization Phase.

in RREP. Finally, the Destination Node sends RREP to Sender Node via neighbor node present in the network. This mechanism is depicted in Figure 4.

4.3 Hash Generation at Source

The Sender Node receives RREP from Destination Node; it extracts the hash code appended in reply and assigned in D_HC (Destination Hash Code) which is generated at destination. And it generates new hash code with same secret key by using the formula explained in the second phase (Hash Generation at Destination). This new hash code is assigned in S_HC (Source Hash Code) which is generated in source. Finally, it compares the received hash value (D_HC) and newly generated hash value (S_HC). If the sender and the receiver hash value matches, the node is treated as legitimate node. Otherwise, the node is treated as selfish node. This is illustrated in Figure 5.

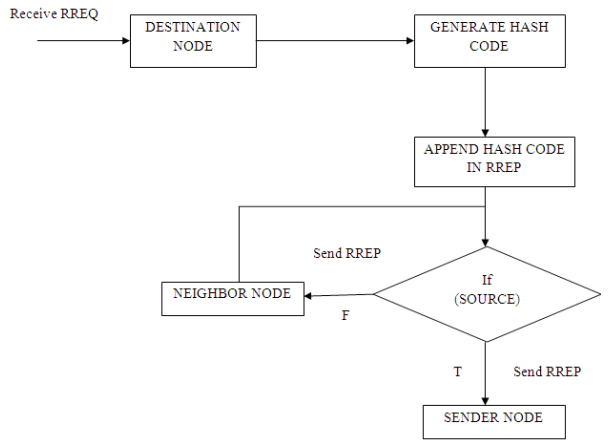

Figure 4. Hash Generation at Destination.

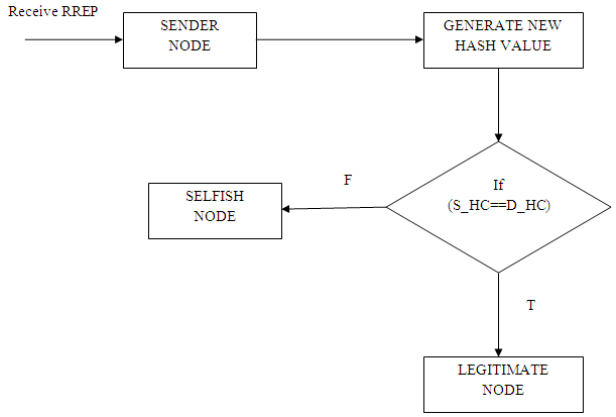

Figure 5. Hash Generation at Source.

4.4 Node Misbehavior Identification and Packet Forwarding Phase

The packet forwarding phase takes place only when the node is legitimate. If the node (Source/Neighbor) is legitimate, it forwards the packet to Destination Node. Else, it sends the Node Misbehavior Notification (NMN) Message to entire nodes present in the network. This is shown in Figure 6.

Algorithm

Input:
N= Number of Nodes
SN = Sender Node
DN = Destination Node
SFN = Selfish Node
S_HC =Sender Hash Code
D_HC =Destination Hash Code
NMN = Node Misbehavior Notification

1. Start
2. SN Sends RREQ to next node
3. If (Destination)
   Sends RREP to source
   SN sends Packet to DN
4. Else if (neighbor node)
   Checks its RT that has route to DN
   Then sends RREP to SN
   SN sends packet to DN
5. Else
   It forwards RREQ to next neighbor node until reach destination
6. After getting RREQ, the hash code is generated by using hash technique with the secret key.
7. Assign the generated hash code to S_HC
8. Hash code is append in RREP
9. DN sends the RREP to SN.

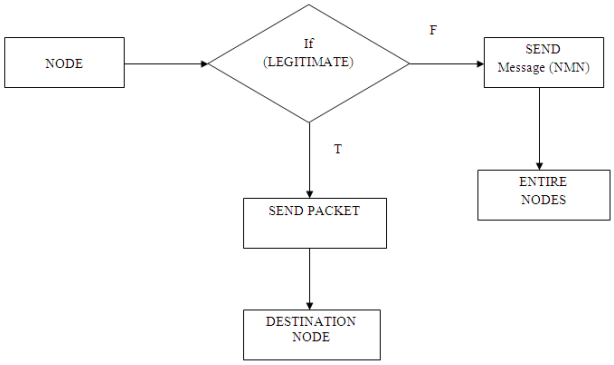

Figure 6. Node Misbehavior Identification.

10. Upon receiving the RREP in source, it generates hash code by using hash technique with the secret key
11. Assign the generated hash code to D_HC
12. If (S_HC == D_HC)
    The node is legitimate node
13. Else
    The node is selfish node (Misbehavior Node).
14. SN sends NMN message to every node present in network
15. Stop

5. Performance Analysis

The proposed algorithm uses the concept of hash function and implemented under the protocol DSR called as hash based DSR. The hash based DSR gives better results compared with the original DSR. The results achieved from simulation testing implemented in MATLAB to study the effect of selfish nodes presents in the network and to evaluate the network performance in terms of throughput and delay.

5.1 Packet Delivery Ratio (PDR)

The ratio between numbers of packets is received in destination and the numbers of packets is sent by the source. Figure 7 shows the comparison of network performance in terms of Packet delivery ratio. The simulation was carried out with the assumption of selfish nodes as 0, 5, 10, 15, 20, 25, 30, 35, 40 and also compares the packet delivery ratio of the original DSR with the proposed hash-based DSR. The percentage of selfish nodes presents in the network various from 0 to 40%. The packet delivery ratio decreases as the number of selfish nodes increases in the network. When compared with the original DSRs, the proposed hash-based DSR preserves a comparatively high packet delivery ratio.

5.2 Delay

The amount of time taken to identify node misbehavior from source to destination is called delay. Figure 8 shows the comparison of network performance in terms of delay. The assumption of selfish nodes as 0, 5, 10, 15, 20, 25, 30, 35, 40 and also it compares the delay of the original DSR with the proposed hash-based DSR. The proposed hash-based DSR comparatively reduces the delay compared with the original DSR.

6. Conclusion

The proposed algorithm uses cryptographic hash function to generate the hash code and the code is appended in RREP instead of appending the hash code in RREQ. As a result, this algorithm works in an efficient way. The message is authenticated by implementing hash based technique. The original message is not been altered by any intruder. The performance of proposed algorithm gives better performance than existing DSR which takes more time to detect the behavior of a single node and also relatively the packet delivery ratio is low. This paper utilizes hash code generated by hash technique to identify the behavior of node under DSR protocol. In future, it may apply to identify the node behavior under AODV protocol and analyze the performance of selfish node present in network.

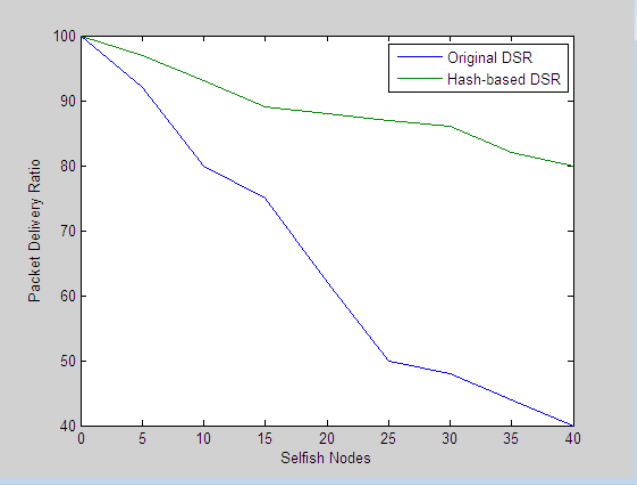

Figure 7. Packet Delivery Ratio.

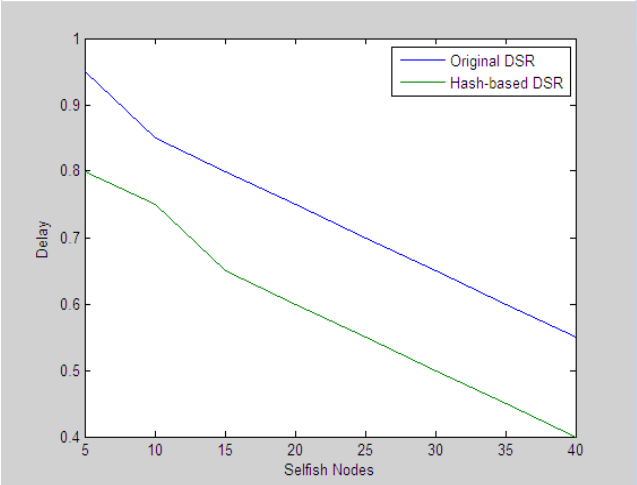

Figure 8. Delay.

7. References

1. Samba P, Aswini M, Kusuma T, Vasudha Y. Detection of Routing Misbehavior Nodes Using Improved 2-ACK in MANET'S (Simulation through NS-2). International Journal of Computer Science and Information Technologies. 2014; 5(2):1042–4.
2. Vennila G, Arivazhagan D, Manickasankari N. A Survey of Sinkhole Attack on DSR in MANET. International Journal of Computer Science and Mobile Computing. 2014 May; 3(5):239–44.
3. Vennila G, Arivazhagan D, Manickasankari N. Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm. International Journal of Engineering and Technology (IJET). 2014 Oct-Nov. 6(5):2401.
4. Padiya S, Pandit R, Patel S. Survey of Innovated Techniques to Detect Selfish Nodes in MANET. International Journal of Computer Networking. 2013 Mar; 3(1):221–30.
5. Koshti D, Kamoji S. Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks. IJSCE. 2011 Sep; 1(4).
6. Goyal P, Parmar V, Rishi R. MANET: Vulnerabilities, Challenges, Attacks, Application. International Journal of Computational Engineering & Management. 2011 Jan; 11:32–7.
7. Thakare AN, Joshi MY. Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks. IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs. 2010.
8. Bai R, Singhal M. DOA: DSR over AODV Routing for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing. 2006 Oct; 5(10).
9. Liu K, Deng J, Varshney P, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehavior in manets. IEEE Transactions on Mobile Computing. 2006; 6(5):536–50.
10. He Q, Wu D, Khosla P. Sori: A secure and objective reputation based incentive scheme for ad-hoc networks. WCNC; 2004. p. 825–30
11. Buchegger S, Boudec JL. Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks). Proceedings IEEE/ACM Workshop on (MobiHoc'02); 2002 Jun. p. 226–336.
12. Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. CMS'02; 2002 Sep.
13. Marti S, Giuli T, Lai K, Bakar M. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00); 2000 Aug. p. 255–65.