RBMD: Reward Based Malicious Detection in Mobile Ad hoc Network

R. Preethi and Dr. M. Sughasiny

Abstract— In Mobile Ad-hoc Network (MANET), the mobile node transmits message directly to another node or via some intermediate nodes. In order to broadcast the messages, the nodes are interconnected to each other using some routing protocols. The communication medium may be not safe and the transmitted data over the nodes can fall into malicious activity. Compared to wired networks, Wireless networks are not secure. The mobile node has limited resources like limited battery power. Due to this reason, the intermediate nodes may acts as a selfish node or malicious nodes which does not forwards any message or modifies and forwards them. To tackle this problem this paper proposed, Reward Based Malicious Detection (RBMD) Algorithm. This algorithm detects two types of attacks, namely, Packet Modifying Attack and Packet Hiding Attack. A Malicious intermediate node modifies incoming packet and forwards to next node is Packet Modifying Attack. A Malicious intermediate node hides incoming packet then keeps no response is Packet Hiding Attack. Each source node provides some reward amount for an intermediate node which detects nearest malicious node using RBMD Algorithm. The experimental results show the proposed RBMD Algorithm detects malicious node in MANET efficiently.

Keywords: Malicious, Battery Power, Intermediate Nodes, Rewards.

1 Introduction

Mobile Ad-hoc Network (MANET) is a collection of independent mobile nodes network which is created, operated and managed by the nodes themselves [1]. MANET nodes have equipment for transmit and receive packets. MANET is not having any infrastructures. Each mobile node has limited coverage area and limited battery power.The mobile node transfers packet directly to another node or through some intermediate nodes [2]. In order to exchange the packets, the nodes are interconnected to each other using some protocols working at different layers.

The communication medium of MANET is totally unsecure. So, the transmitted packet suffers from malicious activities. Compared with wired network, wireless mobile ad hoc network is unsecure.Mobile nodes itself acts as router in MANET. Any node can join or leave network at any instance. So, attacker nodes can be in the MANET independence.

In existing some routing protocols are developed such as AODV, DSR. The researchers enhance these routing protocols to detect malicious activities.The mobile nodes in the MANET are self configuring and do not have a centralized system. They are easily deployable and most of the nodes are migrating. Due to this there exist some malicious nodes which cause mainly two types of attacks namely, Packet Modifying Attack and Packet Hiding Attack.

To deal with this problem, this paper proposed Reward Based Malicious Detection (RBMD) Algorithm. This algorithm detects malicious node efficiently in MANET. Using this algorithm, an intermediate node can detects nearest malicious node and inform about malicious node to source node. After malicious detection the source node remove this malicious node from its Minimum Cost Routing Path (MCRP). Followed by, it provides reward amount to informed intermediate node.

The rest of the paper is organized as follows: Section 2 presents a related work of existing malicious detection techniques. Section 3 describes the proposed Reward Based Malicious Detection Algorithm briefly. Section 4 provides extensive experimental results to support the proposed RBMD algorithm. Finally, Section 5 provides the conclusion of the work.

2 RELATED WORKS

This section describes a related work of existing malicious detection techniques.

Vishnu k. et al. [3] proposed a technique for detection and removal of cooperative black/gray-hole attack in mobile ad-hoc networks. According to their technique, a backbone network of trusted nodes is established over the ad-hoc network. The source node sometimes requests one of the strong energy nodes for a restricted IP address. So the gray/black-hole nodes forward RREP to source node for restricted IP. If any node responds with RREP for restricted IP, the source node consider it is may be malicious.

G.S. Mamatha et al. [4] have proposed a scheme to identify parallel different types of attacks in MANETs. This scheme has 3 phases. First is sender phase, second is intermediate phase and third is receiver phase. This scheme has two way communication and ACK approach. For detect packet dropping, hash code concept is used.

————————————————

- *Preethi. R is currently Research Scholar in Department of Computer Science, Srimad Andavan Arts College, Trichy, TamilNadu, India. E-mail: preethihcc@gmail.com*
- *Dr. M. Sughasiny is currently Assistant Professor in Department of Computer Science, Srimad Andavan Arts College, Trichy, TamilNadu, India. E-mail: drsugha@andavancollege.ac.in*

Anju K. Gupta et al. [5] have given an overview of a wide range of existing protocols focusing on their characteristics and functionality. Based on routing methodologies these protocols are compared.

Ahmed Nabet et al. [6] have proposed an efficient secure routing protocol, ASRP, to ensure the routing security in ad-hoc networks. This protocol provides strong security extensions to reactive AODV protocol.

Radhika Saini et al. [7] a scheme for detect the malicious activities of the sensor node and defense solution to protect packet transmission.

Security solutions include cryptography, protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP).

Robinpreet Kaur et al. [8] have presented different routing protocols proposed in literature and comparison among these protocols through simulations based on certain parameters like throughput, routing overhead, average delay, packet delivery ratio and scalability.

Rajib Das et al. [9] have given an algorithm for investigating and enhancing the AODV protocol's security in opposition to black hole attack.

Based on this algorithm, an extra path to the intermediate node is implemented that answers the more request packet to verify whether the path from the intermediate node to the destination node available or not.

Followed by, against black hole attack in MANET, Shashank Khare et al. [10] have proposed a Secure Ad- hoc On- Demand Distance Vector routing protocol (SAODV) proposed. This protocol is an enhanced version of AODV Routing Protocol. It detects malicious node based on timeout values.

Onkar V. Chandure et al. [11] have proposed a mechanism for the detection and prevention of gray-hole attack in mobile ad-hoc network using AODV protocol. This protocol maintains DRI table for each neighbor nodes.

Shobha Arya et al. [12] have proposed an algorithm for detecting malicious nodes in mobile ad-hoc networks. Encryption, Decryption and ACK approaches are used to provide security. It provides security against 4 types of attacks namely, Black hole attack, gray-hole attack, message tampering attack and packet eavesdropping attack.

Administrator and Trust Based Secure Routing (ATSR) are proposed by Arnab Banerjee et al. [13] in MANET.

Using some parameters, an integer value and trust the ATSR scheme provides secure routing with integrity and confidentiality.

3 REWARD BASED MALICIOUS DETECTION:

For malicious node detection in Minimum Cost Routing Path (MCRP), this section proposed Reward Based Malicious Detection (RBMD) Algorithm. This algorithm detects Packet Hiding Attack and Packet Modifying Attack. Figure 3.1 shows Packet Hiding Attack.

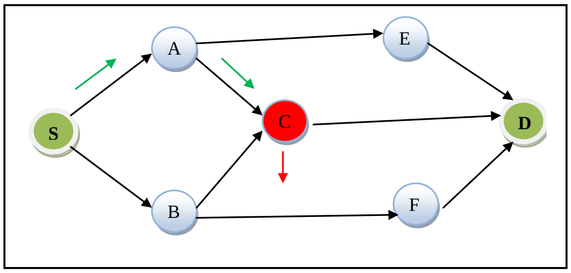


Figure 3.1: Packet Hiding Attack

Followed by, Figure 3.2 shows Packet Modifying Attack.

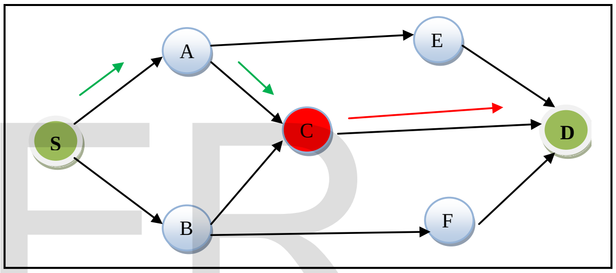


Figure 3.2: Packet Modifying Attack

Figure 3.3 shows Flow Chart of RBMD Algorithm. This algorithm detects malicious nodes using some reward amount providing. Algorithm 1 shows RBMD algorithm briefly.

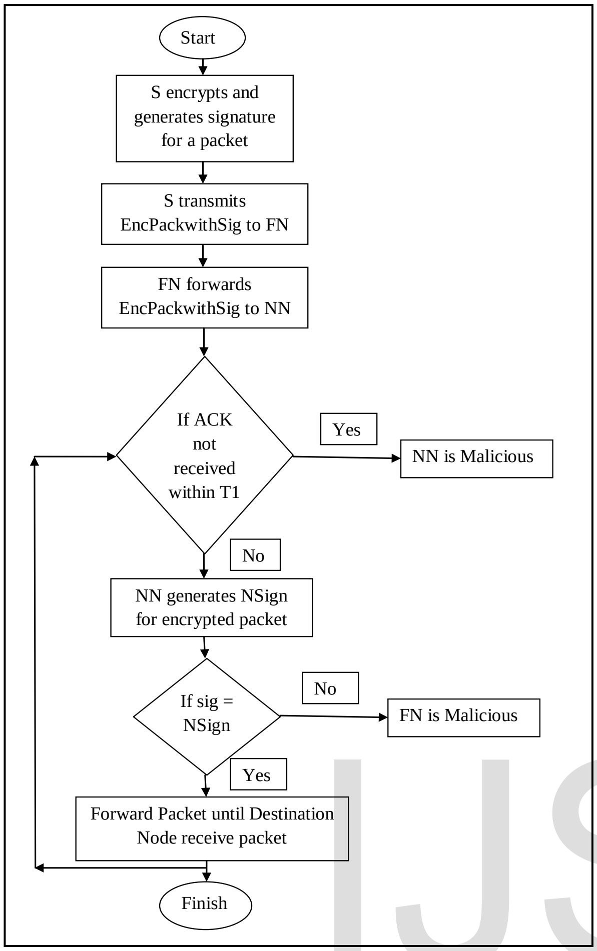

Start
S encrypts and generates signature for a packet
S transmits EncPackwithSig to FN
FN forwards EncPackwithSig to NN
If ACK not received within T1
Yes
NN is Malicious
No
NN generates NSign for encrypted packet
If sig = NSign
No
FN is Malicious
Yes
Forward Packet until Destination Node receive packet
Finish

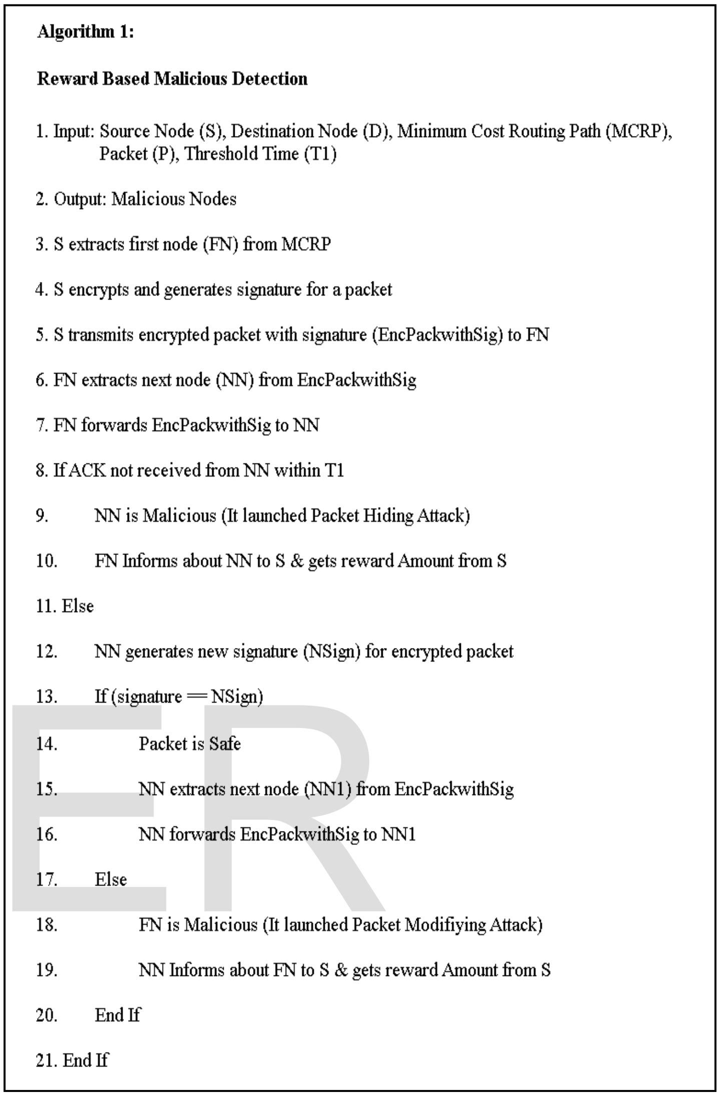
Figure 3.3 Flow Chart of RBMD Algorithm

In MANET, a source node (S) desires to send the packet to the destination node. So it finds Minimum Cost Routing Path. Followed by, it generates public key with secret key. Then it sends the secret key to destination through Secret Sharing.

Source node extracts first node from MCRP (Step 3). Followed by it encrypts a file based on public key, it provides cipher text. Furthermore, it generates signature for cipher text (Step 4).

Source node transmits cipher text with signature to next node FN (Step 5). FN extracts next node NN (Step 6) from MCRP. Followed by, FN forwards cipher text with signature to NN (Step 7). Then FN waits within T1 time for receive acknowledgement message from NN. If acknowledgement message not coming within T1 time the NN is Malicious.

Because it launched packet hiding attack (Step 8 & 9). FN informs the status of NN to S and gets rewards from S (Step 10). If acknowledgement message received in FN, NN generates new signature for received cipher text and compare received and new signatures are same or not.



```
Algorithm 1:

Reward Based Malicious Detection

1. Input: Source Node (S), Destination Node (D), Minimum Cost Routing Path (MCRP),
          Packet (P), Threshold Time (T1)
2. Output: Malicious Nodes
3. S extracts first node (FN) from MCRP
4. S encrypts and generates signature for a packet
5. S transmits encrypted packet with signature (EncPackwithSig) to FN
6. FN extracts next node (NN) from EncPackwithSig
7. FN forwards EncPackwithSig to NN
8. If ACK not received from NN within T1
9.      NN is Malicious (It launched Packet Hiding Attack)
10.     FN Informs about NN to S & gets reward Amount from S
11. Else
12.     NN generates new signature (NSign) for encrypted packet
13.     If (signature == NSign)
14.           Packet is Safe
15.           NN extracts next node (NN1) from EncPackwithSig
16.           NN forwards EncPackwithSig to NN1
17.     Else
18.           FN is Malicious (It launched Packet Modifiying Attack)
19.           NN Informs about FN to S & gets reward Amount from S
20.     End If
21. End If
```

If both are same (Step 13), FN is normal node otherwise FN is malicious node (Step 18). Because, FN launched Packet Modifying Attack. NN informs the status of FN to S and gets rewards from S. Forward packet through remain nodes in MCRP then finally Destination node (D) receives packet. Followed by, D generates new signature for received packet and checks both signature are same or not. If both are same it decrypts packet based on secret key.

4 Experimental Results:

This section presents experimental results in terms of some evaluation parameters namely Packet Delivery Ratio (PDR) and Energy consumption (EC). It shows the proposed RBMD algorithm achieves superior performance.

4.1. Packet Delivery Ratio:

Packet Delivery Ratio determines the percentage of packets correctly received at the destination node divide by number of packets sent from the source node.

PDR = (number of packets correctly received / total number of packets transmitted from the source node) * 100%

The Packet Delivery Ratio values between 0-100 only.

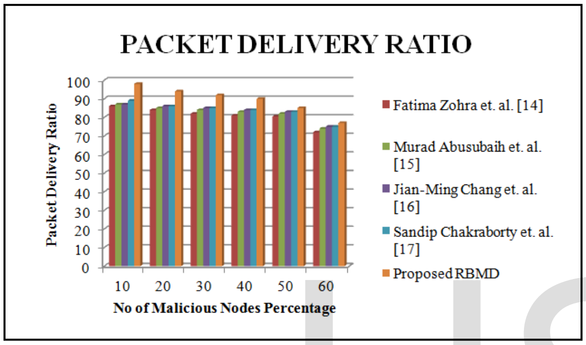


Figure 4.1 Packet Delivery Ratio comparisons

Compared with others, proposed RBMD algorithm's Packet Delivery Ratio is very high which is showed in Figure 4.1

4.2 Energy Consumption:

In MANET, Energy Consumption is one of the important metric. While each nodes receiving and transmitting energy consumption is computed. A node which is in idle, it is not consumes any energy. The powers for transmission and receiving are fixed values, 0.6 J and 0.3 J, respectively. When a mobile node sends Packet (P) to next node, the node's energy capacity will be decreased by following equation.

EC = Er + (Dist * PS * Et)

EC is the Energy Consumption of a node in J; Dist is the distance between a node to next node in meter and PS is the Packet Size in Kb. In this way a node's energy consumption is calculated.

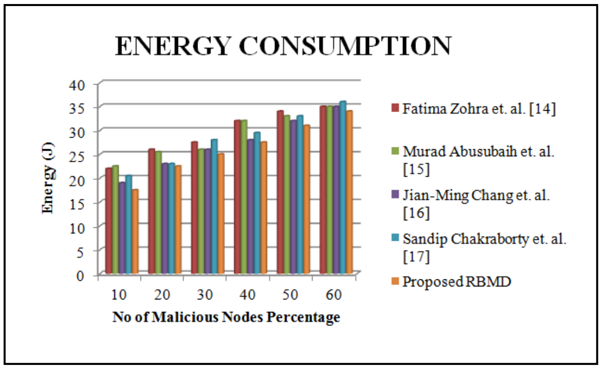


Figure 4.2 Energy Consumption comparisons

Compared with others, proposed RBMD algorithm's consumes less energy which is showed in Figure 4.2.

5 Conclusion:

This paper proposed a Reward based Malicious Detection (RBMD) algorithm for identifies the malicious nodes and removes them in routing. This algorithm identifies malicious nodes based on packet hiding attack and packet modifying attack detection. Furthermore, the intermediate nodes earn rewards for identifying nearest malicious nodes. This algorithm takes shortest trusted path for reduce energy consumption. Experimental Results shows proposed RBMD algorithm has less energy consumption for packet transmission compared with others. Furthermore, this algorithm detects malicious nodes efficiently.

References:

[1] S. Corson and J. Macker, Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC Editor, 1999.

[2] Giordano, S. (2002), "Mobile ad hoc networks" Handbook of wireless networks and mobile computing, 325-346.

[3] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.

[4] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETs", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October 2010.

[5] Anuj K. Gupta, Harsh Sadawarti and Anil K. Verma, "Review of Various Routing Protocols in MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.

[6] Ahmed Nabet, Rida Khatoun, Lyes Khoukhi, Juliette Dromard and Dominique Gaiti, "Towards Secure Route Discovery Protocol in MANET", Conference Publication, August 2011.

[7] Radhika Saini and Manju Khari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", International Journal of Computer Applications, Vol. 20, No. 4, April 2011.

[8] Robinpreet Kaur and Mritunjay Kumar Rai, "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal, Vol. 1, ISSN: 2278-1129, 2012.

[9] Rajib Das, Dr. Bipul Syam Purkayastha and Dr. Prodipto Das, "Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology, Vol. 3, No. 4, pp- 2832-2838, ISSN: 0975-5462, April 2012.

[10] Shashank Khare, Manish Sharma, Namrata Dixit and Sumit Agarwal, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET", VSRD International Journal of Electrical, Electronics and Communication Engineering, Vol. 2 (6), pp- 385-390, ISSN: 2231-3346, 2012.

[11] Onkar V. Chandure and V.T. Gaikwad, "Detection and Prevention of Gray Hole Attack in Mobile Ad- Hoc Network using AODV Routing Protocol", International Journal of Computer Applications, Vol. 41, No.5, ISSN: 0975- 8887, March 2012.

[12] Shobha Arya and Chandrakala Arya, "Malicious Node Detection in Mobile Ad- Hoc Networks", Journal of Information Operations Management, Vol. 3, pp- 210- 212, ISSN: 0976-7754, January 2012.

[13] Arnab Banerjee, Dipayan Bose, Aniruddha Bhattacharyya, Himadri Nath Saha and Dr. Debika Bhattacharyya, "Administrator and Trust Based Secure Routing in MANET", International Conference on Advances in Mobile Network, Communication and its Applications, 2012.

[14] Fatima Zohra, M., Maaza Zoulikha, M. and Said, K. (2011) Techniques of Detection of the Hidden Node in Wireless Ad Hoc Network. Proceedings of the World Congress on Engineering, 2, 978-988.

[15] Abusubaih, M. (2011) A Combined Approach for Detecting Hidden Nodes in 802.11 Wireless LANs. Annals of Telecommunications. Annales des Telecommunications, 66, 635-642.

[16] Chang, J.-M., Tsou, P.-C., Woungang, I., Chao, H.-C. and Lai, C.-F. (2015) Defending against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach. IEEE Systems Journal, 9, 619-621.

[17] Chakraborty, S., Nandi, S. and Chattopadhyay, S. (2016) Alleviating Hidden and Exposed Nodes in High-Throughput Wireless Mesh Networks. IEEE Transactions on Wireless Communications, 15, 928-937.