International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

A Novel Security Approach For Mitigating Packet Dropping Attack In Mobile Ad Hoc Networks

Ranjeeth Kumar Sundararajan[1], Sivanesan.P [2], James Manoharan.J [3]

[1]*Assistant Professor, Department of Computer Applications, Bishop Heber College, Tiruchirappalli – 620 017.*
[2]*Assistant Professor, Department of Information and Communication Technology, SASTRA Deemed University, Thanjavur – 613 401.*
[3]*Associate Professor&Head, Department of Computer Applications, Bishop Heber College, Tiruchirappalli – 620 017.*

Abstract: A Mobile Ad hoc Network (MANET) also known as wireless ad hoc network is an increasingly self-building, framework less network of mobile devices combined wirelessly. MANET is a decentralized environment. In such decentralized environment, network nodes perform packet forwarding and other routing services without any central administration. Some security threats like sinkhole attack, black hole attack etc., may occur in the decentralized environment. To address this problem, we propose a novel security approach to detect the malicious node and retransmit the packets into new secure route. In the existing system, Bernoulli Bayesian model is adapted for node's behavior classification and Markov Chain model is used for behavior evolution tracking. The proposed system adapts node behavior classification using behavior vectors for detecting the malicious nodes and re-route the packet. The proposed system adapts Dijkstra's shortest path algorithm for sending the packet to the nodes and identifies the malicious nodes earlier that increases the security of the MANET.

Keywords: Mobile Ad hoc Network (MANET), Bernoulli Bayesian, Markov Chain model, Dijkstra's shortest path algorithm

1. INTRODUCTION

1.1. Overview:

Mobile ad hoc network is a dynamic network that can build up the location and change itself. Because MANETs are mobile devices, that are connected to various networks through the wireless connection. Efficient network connectivity is provided in wireless communication technology when compared to wired networks. MANETs are network of people, they dynamically formed and allow people in a restricted area to transfer, catch and measure data without the need of either framework or centralized support [1]. Mobile ad hoc networks are made up of small portable devices that are combined using wireless links. These networks have no fixed framework and there is no centralized supervising structure like base station [2].

In such decentralized environment packet forwarding, route discovery, route establishment and route maintenance are accommodated by network nodes together without any central administration. However, security is not considered to sketch out in most of the existing routing protocols. An intruder can easily distract the routing process by inserting fake control messages, breaking the routes of packets or also dropping collected packets [3]. This attack is performed by malicious node. When the communication route is established between source and destination node, the malicious node appears in between the source and destination node to drops packets [4]. Malicious nodes behave as a legitimate node and extract the vulnerabilities of the routing protocols which leads to crash entire network [5].
In the proposed work packet dropping attack in mobile ad hoc network is mitigated and packets are rerouting through the new secure route. Performance analysis and results are obtained using MATLAB simulation environment.

1.2. Type of attacks

Table 1: Type of attacks

S. No	**Attacks**	**Description**
1	Eavesdropping	Eavesdropping is the un-justified real-time interference of a privacy conversation such as a phone call, prompt message, video conferencing or tax transposal.
2	Data modification	An attacker modifies the data on a target machine.
3	Identify spoofing	A spoofing attack is a situation in which one person or program profitably acts like an authorized user through falsifying data by that gaining an untrustworthy leverage.
4	Password-based Attack	Duplicate a valid logon or password sequence is made by a repetitive attempt.
5	DOS attack	It is a cyber-attack, which can prevent the accessing rights of the resources from the legitimate user.
6	Man-in-the-middle Attack	Two parties communicate with each other who believe that they are directly communicating, but the attacker secretly alters the communication between them
7	Compromised-key Attack	An attacker has a compromised key to access an information of authorized persons (sender and receiver) without the knowledge of sender and receiver.
8	Sniffer attack	A sniffer is an application which is used to read the data within the network packets even if they are not encrypted.

1.3. Literature survey

Table 2: Related works

S. No	Paper Title	Year of published	Concept
1	Detecting Attacks In MANET using secure zone routing protocol.	2017	Author propose a new mechanism called enhanced OLSR(optimized link state routing) protocol to analyze the vulnerabilities of routing protocol and secure the nodes against the attacks [6].
2	Survey of effect of packet dropping attack in AODV routing and Detection of such nodes in MANET.	2016	In this paper authors compares all the detection techniques and how they detect the misbehavior link and malicious node to prevent from packet dropping attack [7].

3	Review of a secure approach to prevent packet Dropping and message tampering Attacks on AODV-based MANETs.	2015	Different approaches are handles to provide a security in network layer. It helps to detect and prevent from packet dropping attack, wormhole attack, black hole attack and message tampering attacks in MANET [2].
4	BlackholeDetectionandpreventionusingAODVandshortestdistanc etechnique.	2017	A fidelity table is maintained to measure a reliability of every node in the network. Based on the fidelity level nodes behavior is classified [8].
5	A survey on contemporary MANET security: Approaches for securing the MANET.	2017	Two security levels such as cryptography method and IDS mechanism. Cryptography method is to secure the data transmission. Second one is to monitoring the node [9].

6	Active detection in mitigating routing misbehavior for MANETs.	2017	Explore based active detection (EBAD) mechanism is effectively mitigate the routing misbehaviors in MANETs [10].
7	A survey paper on preventing packet dropping attack in mobile ad-hoc network.	2017	Node bypassing technique issued to detect and remove the malicious nodes from the network [11].
8	Detection of Wormhole, Black hole and DDOS attack in MANET using trust estimation under fuzzy logic methodology.	2017	In this paper a trust value of each node in the network is calculated and applies fuzzy logic to detect worm hole, Black hole and DDOS attack in MANET [12].

9	A survey on detection of packet dropping attacks in wireless ad hoc network.	2015	In this paper, dynamic source routing (DSR), Ad-hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR) protocols and various detection methods are used to detect and isolate packet drops [13].
10	A review on trust and security by using intrusion Detection system in mobile ad hoc network.	2017	In this paper, intrusion detection system is used which is a process of monitoring the entire network Regularly for detecting the malicious node and attaining the security [14].

2. SYSTEM ANALYSIS

2.1. Existing system

In the existing system, a novel detection mechanism is proposed to detect the different patterns of packet dropping attacks. A novel detection mechanism includes Bernoulli Bayesian model, fuzzy logic model and Markov chain model. The Bernoulli Bayesian model is used for node behavior classification, it provides some probability value for each node that participates in the network. Based on the probability value the node behavior is classified. Obtained probability value is applied to fuzzy logic model to identify the maliciousness level

that is assigned to the state of a node. Finally, Markov chain model is used to predict the stationary state based on its behavior evolution tracking.

2.2. Drawbacks of Existing System

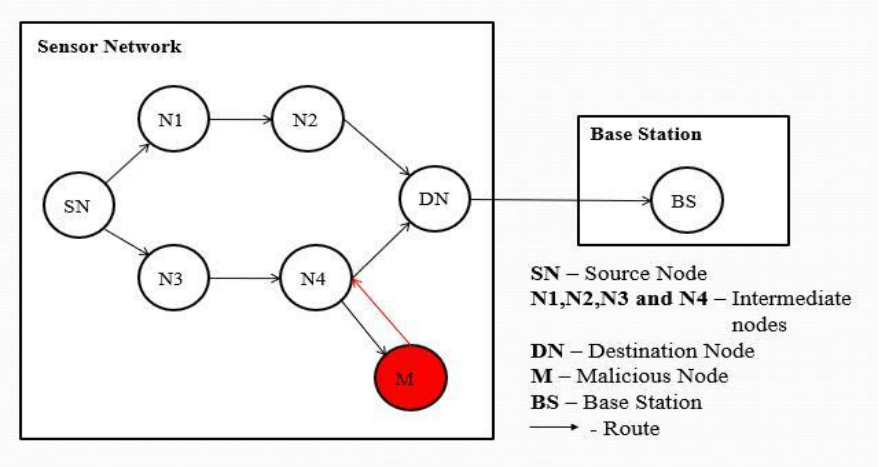
In the existing system, it is designed only to detect the packet dropping attacks, there is no focus to find new secure route to retransmit the packet. Behavior-based prediction process takes more time to detect the attack, because of using more number of states. The system had not focused on evaluation metrics like node energy level, throughput and network delay.

2.3. Proposed system

In proposed work, Dijkstra's algorithm is used for shortest path discovery between source and destination node. Once the route is established between source and destination node, then the detection mechanism is applied to detect for malicious nodes appearing in that route. In our security approach the packet dropping attack is effectively mitigated and discovered new secure route to retransmit the packets.

2.4. System Architecture

The system architecture is depicted as follows.



2.1 System Architecture

Algorithm: Behavior Vector based Detection Process

Input: Node SN tracks the behavior of N1 {collecting information about packet forwarding}

P[3] ⟵ (RREQ,RREP,DATA);

For (i=1; i<=3; i=1+1)

If (p[i]==1) then

P[i] ⟵ legitimate;

Else

P[i] ⟵ malicious;

End

End

Mal[3] ⟵ (1,0,0);

Leg[3] ⟵ (1,1,1);

{Detection of malicious behavior}

If (p == Leg) then

Print “Legitimate Behavior”;

Else if (p == Mal) then

Print “Malicious Behavior”;

End

Output: Malicious Node ID

2.4.1 Algorithm Description

Our security approach is effective in detecting the packet dropping attack and discovers new secure route to retransmit the packets. Using such approach misbehavior nodes cannot deceive our detection system. Detection mechanism is strongly constituted in the following module diagram.

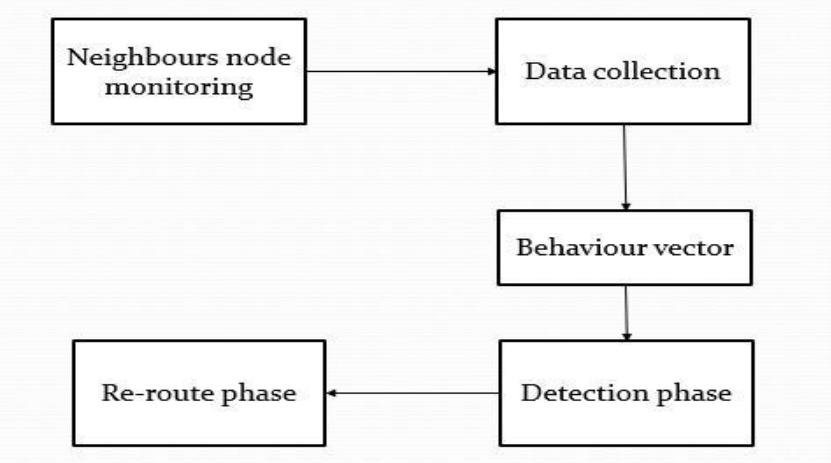


Figure 2.2 Detection Mechanism Module

Data collection phase: Each node in the network monitors its neighbour node in order to collect information about packet passed by its 1-Hop neighbors.

Behavior classification phase: Based on the data collection phase each neighbor node composes behavior vector. Node behavior is classified based on the obtained behavior vector.

Detection phase: Obtained behavior vector is used to detect the malicious node in the network.

Rerouting phase: It is a final phase to discover new secure route to retransmit the packet. Rerouting path is fully secured for retransmitting the packet.

3. CONCLUSION AND FUTURE ENHANCEMENT

3.1. Conclusion

In this paper, a decentralized approach is adapted to mitigate packet dropping attack in Mobile Ad Hoc Network. The detection at a particular node starts by monitoring the behaviors of 1-hop neighbors in order to collect information about the exchanged packets and constructs their behavior vector. Based on the behavior vector, the malicious nodes are detected and packets are retransmitted through new secure route without the presence of malicious nodes. The efficiency of the system will be proved through extensive simulations for detecting packet dropping attacks with an expected accuracy rate greater than 95%.

3.2. Future Enhancement

In future work, the algorithm will be experimented using a simulator and results will be analyzed. Further the packet dropping attacks in the Internet of Things (IoT) environment can be analyzed. Since the IoT is playing a major role in building smart applications, the security is of major concern. So, it is necessary to give more focus to provide secure IoT environment.

4. REFERENCES

[1] M. Rmayti, R. Khatoun, Y. Begriche, L. Khoukhi, and D. Gaiti, "A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks,"*Computer Networks*, vol. 121, pp. 53–64, 2017.

[2] A. A. Morey and J. W. Bakal, "Review of a Secure Approach to Prevent Packet Dropping and Message Tampering Attacks on AODV-based MANETs,"*International Journal of Computer Science & Information Technologies*, vol. 6, no. 3, pp. 2373–2376, 2015.

[3] R. Khatoun, L. Khoukhi, A. Nabet, and D. Gaïti, "Asrop : Ad Hoc Secure Routing Protocol," *Int. J. Wirel. Mob. Networks*, vol. 4, no. 5, 2012.

[4] R. Khatoun, Y. Begriche, J. Dromard, L. Khoukhi, and A. Serhrouchni, "A statistical trust system in wireless mesh networks," *Ann. des Telecommun.* vol. 71, no. 5–6, pp. 187–199, 2016.

[5] T. K. Shanida and S. Karunan, "Packet Dropping in Wireless Ad Hoc Networks," pp. 55–60, 2017.

[6] K. Murali, M. Rahul, G. Venkateshwaran, and S. Pariselvam, "Detecting Attacks in MANET using Secure Zone Routing Protocol," vol. 7, no. 4, pp. 10182–10185, 2017.

[7] N. Soliyal, "Survey of effect of packet dropping attack in AODV routing And detection of such nodes in MANET," vol. 6, no. 2, pp. 96–101, 2016.

[8] M. Y. Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,” *Comput. Commun.*, vol. 34, no. 1, pp. 107–117, 2011.
[9] I. Journal, “A Survey on Contemporary MANET Security : Approaches for Securing the
MANET A Survey on Contemporary MANET Security : Approaches for Securing the,” no. April, 2017.
[10] C. Pu, S. Lim, J. Chae, and B. Jung, “Active detection in mitigating routing misbehavior for MANETs,” *Wirel. Networks*, 2017.
[11] R. Arthi, S. I. S. P, and R. Kirubakaran, “A Survey Paper on Preventing Packet Dropping Attack in Mobile Ad-Hoc MANET,” vol. 2, no. 2, pp. 818–821, 2017.
[12] A. K. Khare, “Detection of Wormhole , Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology,” no. July, pp. 29–35, 2017.
[13] K. Shridevi and N. Parveen, “A Survey on Detection of Packet Dropping Attacks in Wireless Adhoc Network,” vol. 4, no. 6, pp. 52–56, 2015.
[14] R. Gupta and R. K. Paul, “A Review on Trust and Security by using Intrusion Detection System in Mobile Ad Hoc Network,” vol. 6, no. 5, pp. 21236–21240, 2017.