Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.467 – 473

A METHOD TO DETECT PACKET DROP ATTACK IN MANET

Vinod Bhupathi, IT Department, Vardhaman College of Engineering

P Buddha Reddy, IT Department, Vardhaman College of Engineering

G Srikanth Reddy, IT Department, Vardhaman College of Engineering

Abstract: Mobile ad-hoc Network is a self organized spontaneous infrastructure less network which supports networking activities like routing and data transmission. The Data Packets are transferred from one mobile node to another mobile node. The mobile node has a limited resources like limited battery power. Due to this the intermediate nodes may acts as a selfish node or malicious nodes which does not forwards any packet and drops them. In this paper, a mechanism for detection of packet dropping attack is presented based up on the co-operative participation of nodes in a manet.

Keywords: Mobile ad-hoc networks (MANETS), malicious node, Packet Drop Attack.

Introduction:

Mobile Ad-hoc Network is a collection of independent mobile nodes network which is created, operated and managed by the nodes themselves. Manet is a infrastructure less, self-organized and spontaneous network where the nodes helps each other by passing data and control packets from one node to another node. Each mobile node has features like autonomous, limited battery power, dynamic topology etc. The mobile node transfers packet directly to another node or through

some intermediate nodes. In order to exchange the packets, the nodes are inter-connected to each other using some protocols working at different layers (ex: Network layer, Transport layer). The medium of communication or channels may be unsecure and the transmitted data over the nodes can fall into malicious activity. Wireless networks are less secure compared to wired networks. They are created temporary as per requirement or application. Mobile nodes itself acts as router in Manet. Any node can join or leave network at any instance. Hence malicious nodes can be in the network without any detection. Packet dropping through that malicious nodes can be done.

Protocols are used on all the layers to transfer data co-operatively. Some standard routing protocols and customized protocols are developed according to the requirement. The protocols are feasible to detect the malicious activities at routing level.

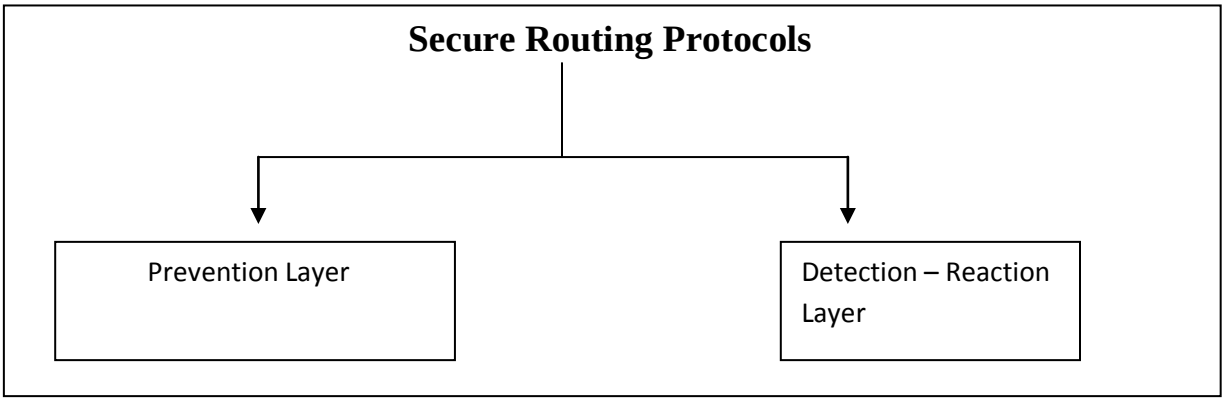
The mobile nodes in the manet are self configuring and does not have a centralized system. They are easily deployable and most of the nodes are migrating. Due to this there exist some malicious nodes which cause different types of attacks such as eves dropping, flooding attack, black hole attack, packet drop attack etc.

This paper presents the solution to packet drop attack and improves the performance of the network. The paper is organized as follows, section II discusses related work on protocols exists in Manets, section III about the packet drop attack problem, section IV about the mechanism to detect the packet drop problem, section V discusses simulation and final section IV concludes the paper and future work.

2. Secure Routing Protocols:

There are multiple classes of routing protocols in MANET to achieve multi-hop routing between any two mobile nodes.

We briefly divide the routing protocols in MANETS into two classes.



Prevention Layer:

- Static
- Standard Protocols
- Authenticated routing for Ad-hoc Networks

Detection – Reaction Layer:

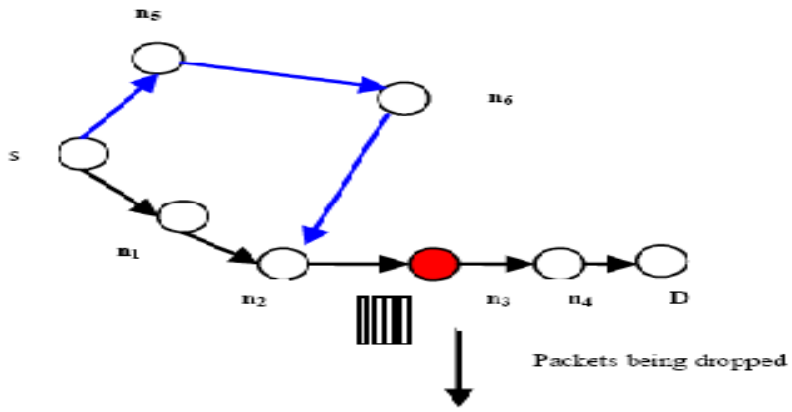
- Dynamic
- Monitoring
- Collaborative Trust based secure routing
- Customized protocols

- Protocols that deploy cryptographic techniques to secure the routing usually remain static during the operation. They are classified as prevention layer protocols or standard protocols.
- Protocols that deploy monitoring technique capture the dynamic events to enhance the protection of the basic operation. They are actually referred as detection – reaction layer and uses some customized protocols based on the situation.

3. Packet Drop Problem:

The main assumption of the ad-hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of packet forwarding. However, the existence of malicious

nodes cannot be disregarded in any system, especially in open networks like mobile ad-hoc networks.



It is an unrealistic anticipation to find all the mobile nodes in an independent network like MANET. The consequence of not forwarding the packets or dropping the packets in a MANET leads to a serious problem. Therefore, the need to address the packet dropping event takes higher priority for the mobile ad-hoc networks.

A packet may be dropped under various reasons, which in turn grouped into various categories.

a. Unsteadiness of the medium
- A packet may be dropped due to confusion in the medium
- A packet may be dropped due to broken link
- A packet may be dropped due to heavy traffic in the media

b. Genuineness of the node
- A packet may be dropped due to overflow of transmission queue
- A packet may be dropped due to lack of energy resources.

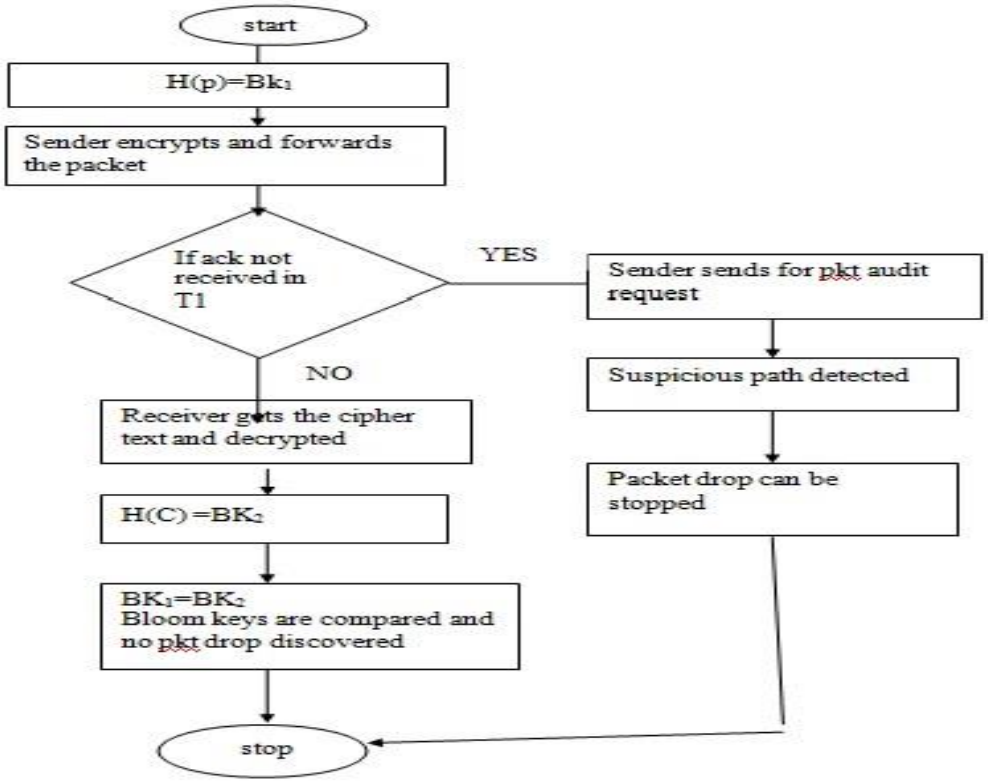
c. Selfishness of the node:
- A packet may be dropped due to selfishness of a node to save its resources.

d. Malicious of the node:
- A packet may be dropped due to malignant act of a malicious node.

4. Detection of packet Drop Problem:

We plan to use a customized packet drop protocol to forward the packets from one node to another node. The sender node initially checks to which node the packet should be forwarded. The node information of each node is known to another node. The sender node usually maintains the sequence number count when a packet is forwarded from one node to another. When a packet is forwarded from one node to another node a sequence number is added. The sender node usually tests the sample packet before forwarding the actual packet being sent.

At first, the sender node calculates the Bloom key(Bk1), encrypts the packet and forwarded to next node. When a packet is forwarded from one node to another node, an acknowledgement should be received in a fixed time T1 and sequence number should be added at sender node. If the acknowledgement is not received in Time T1, the sender node checks for packet audit request. Then the trace file shows the node which drops the packet and the Bloom key (Bk2) is generated after the packet is received. The difference in both the bloom keys also detects the packet drop attack.



P – Packet to be sent

Bk1 – Bloom Key1

Bk2 - Bloom Key2

T1 – Time within the acknowledgement should be received

C - Cipher text of original packet

If the acknowledgement is received to sender in affixed time T1, then there is no packet drop and there is a secured transmission in the network.

5. Simulation:

In this effort, we have tried to show the packet drop attacks in the wireless networks. To attain this we have replicated the wireless ad-hoc network setup which contains packet drop node using NS2 network simulator program. To create the packet drop node in a wireless ad-hoc network, we have employed our own protocol to test.

PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator NS 2.35
Simulation Time	10s, 20s
Number of nodes	10,20,40,60
Transmission Range	250m
Maximum Speed	0-22 m/s
Application Traffic	CBR [constant Bit Rate]
Packet Size	512 bytes
Protocol	Packet Drop
Node Mobility Model	8 Pkts/s

Results:

The comparison of two bloom keys detects the packet drop nodes and also shows the node at which the packet being dropped in the MANET. The change in the bloom key is due to packet drop by the nodes.

6. Conclusion:

We propose a simple yet effective scheme to identify the misbehaving nodes that drops the packet. Each packet is encrypted and bloom key is generated so as to hide the original packet. In the future aspect, we plan to calculate the through put, in order to calculate the performance of the Manet.

References:

[1] Venkatesan Balakrishnan and Vijay Varadharajan, " A serious Threat to Operational Mobile Adhoc Networks", In Proceedings of the 6th International Conference on Mobile Computing and Networking.

[2] Shirini Samreen and Dr. G. Narasimha, "Detection of Colluding Adversaries in a Packet Drop Attack in MANET", In the Proceedings of the International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181

[3] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad–hoc Networks", In the proceedings of the International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2249-8958, Volume-2, Issue-2, December 2012.

[4] N.Bhalaji, Dr.A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", In the proceedings of JOURNAL OF SOFTWARE, VOL. 4, NO. 6, AUGUST 2009.

[5] Angel Mary Alex, M. Ashwin, "Detection of Stealthy Attacks of Packet Dropping in Wireless Ad Hoc Networks", In the proceedings of International Journal of Science, Engineering and Technology Research (IJSETR).

[6] P.Swetha, Vinod Bhupathi, "MITIGATION OF PACKET DROP ATTACK IN MANET", In the proceedings of National Conference on Advances in computing and Networking (NACACN) ISBN:9789383038114.

