Detection and Prevention of Flooding Attack in MANET using Support Vector Machine (SVM)

Sukanya S Gaikwad

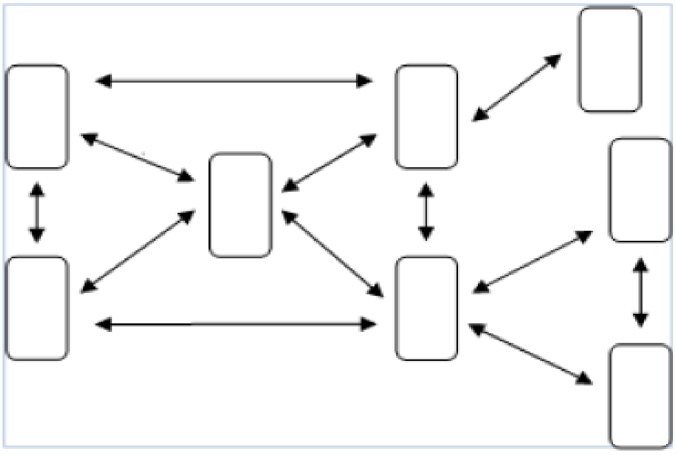
Research Scholar
Department of Computer Science,
Gulbarga University, Kalaburagi, India

Abstract— **Deficiency of infrastructure and dynamic nature of MANET attracts to launch attack, one of them is flooding. Reactive routing for example AODV is more popular than proactive routing as it uses flooding to find out route. In this technique, attackers launch DoS attack like flooding, black hole and gray hole which are the recognized attacks in MANET. In this project, we have proposed a new method based on AODV behavioral metrics detect and prevent MANET flooding attacks. In this method we have used the PDER, CO and PMIR as metrics to prediction of flooding attacks. The proposed method is implemented on NS-2 test bed.**

Index Terms— **Ad-hoc Network; MANET; AODV; SVM; Flooding Attack; NS3; CO; PMP.**

I. Introduction

An ad-hoc network is a local area network (LAN) that is built impulsively as devices connect. Instead of relying on a base station to coordinate the gush of messages to each and every node in the network, the individual network nodes transfer packets to each other.



A MANET is a kind of ad hoc network that can alter locations and configure itself on the soar. Because MANETS are movable, they use wireless connections to join to diverse networks. Mobile ad-hoc networks, also identified as short-lived networks, are independent systems of mobile nodes forming network in the deficiency of any centralized support. Deficiency of fixed infrastructure poses numerous types of challenges for this kind of networking. Among these challenges is routing. In the mobile ad hoc network, nodes can openly communicate with all the other nodes in their radio ranges, while nodes that not in the direct communication range use intermediate nodes to communicate through each other. In MANET, there is forever a quick alter of the topology structure due to the speedy and swift mobility of the movable devices. Topologies of these networks alter recurrently .To solve this difficulty, special routing protocols for MANETs are desired .A number of routing protocols were deliberated, but all fall into three major categories: Proactive, Reactive, and Hybrid routing protocols .Proactive MANET protocols (PMPs) continually revise network topology information and guarantees that it is available to all nodes. Reactive MANET protocols verify routing paths only when necessary. There is no storage of routing tables and no need to analyze best-path scenarios. When a route is required, the system floods the network with route request packets. These are transmitted instantly to connected routers that pass this request for a path to a specified destination. The first reply received determines the path to be used. Hybrid routing protocols are a latest invention of protocols that merge the features of both reactive and proactive routing protocols under diverse scenarios. Mobile Ad-Hoc Network (MANET) is generally susceptible to security attacks due to its characteristics of open medium, dynamic topology, cooperative algorithms, infrastructure less lack of centralized monitoring and management point, and often scarcity of an obvious line of defence. In this paper routing based method has been introduced to detect DoS attack like flooding. The proposed method is based on AODV . AODV is a well recognized and accepted reactive type's protocol used in MANET.

II. Literature Survey

A MANET is a kind of ad hoc network that can alter locations and configure itself on the soar. Because MANETS are movable, they use wireless connections to join to diverse networks. Mobile ad-hoc networks, also identified as short lived networks, are independent systems of mobile nodes forming network in the deficiency of any centralized support. A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers connected by wireless links. The routers are free to move randomly and organize themselves capriciously. Thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion. Each of the nodes has a wireless interface and communicates with its neighbors who are all in its coverage range. Source can reach destination through one or multiple hop.

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol enables multi-hop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is reactive since it does route request only when needed and does not require nodes to maintain routes to destination that are not actively used in communications. Flooding attack in MANET is a more concealed form of DOS attack which is produced by the unintentional failure of nodes in the network or by malicious action. This flooding attack can cause severe degradation in network performance. The main intention of a flooding attack is to interrupt the services given to legitimate users by targeting the resource at the victim node or the network. By consuming the resources like bandwidth, battery power etc attacker can set up the denial of service to the end user. In flooding attack the bogus control packets are flooded into the network targeting the victim or the network as a whole.

With continuous scale-up of the network and increase of the kinds of the services on the network, more and more people pay attention to the modeling and prediction for network traffic. Recently,SVM(Support Vector Machine),a new machine learning method, is comprehensively used to solve the problem of non-liner classification and regression. SVM is a new machine learning method that is put forward by V. Vapnik et al. and based on SLT (Statistics Learning Theory) and SRM (structural risk minimization) is used comprehensively in many fields, including pattern recognition, data mining, text classification, IDS(Intrusion Detection System) and time series prediction. Compared with other learning machine, SVM has some unique merits like small sample sets, high accuracy and strong generalization performance. Standard SVM has a distinct characteristic it usually reflects the low-dimension non-linear object into the linear object in the high-dimension space.

Flooding is a requisite message spreading technique for network-wide broadcast within mobile ad hoc networks (MANETs). Topological awareness is not essential for flooding in MANET. Every the routing protocol is based on the on demand routing is established path via the flooding method. While aggressor used this flooding to interrupt the communication it’s called flooding attacks.

In data flooding, malicious node floods the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of worthless data packets. These useless data packet exhausts the network resources and hence genuine user can not able to use the resources for valid communication.

Author Humaira Ehsan and Farrukh Aslam Khan has been suggested evaluation of network performance for AODV especially in terms of packet efficiency, routing overhead, and throughput. Author Arpita Raverkar has been define three parameter Route discovery, throughput and delay for detection of flooding attack. Author S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam has been used to detect malicious node who floods in the network using RREQ messages, has proposed a statistical approach to avoid the forwarding of such packets via the concept of RREQ counts.

Author Abdur Rashid Sangi, Jianwei Liu and Likun Zou has been discuss about attack has been done by the authorize node. Attacks have been initiated by authenticated nodes/devices in Ad Hoc Network to disrupt the network called byzantine attack. Although these attacks can be initiated independently but are more distressing if start in a mutual way. They highlight the performance degradation of AODV routing protocol, when the byzantine attack are initiated in a combination.

III. Existing System

A MANET is a category of wireless ad hoc network that can change locations and configure itself. These types of networks are without fixed infrastructure and are more prone to attacks that occur in the network.

The main challenge in MANET is to design the robust security. Flooding attack is a kind of Denial of service (DOS) attack which is distributive in nature and can exhaust the victim’s network of resources such as bandwidth and energy etc.

Disadvantages of Existing System:

- The main challenge in MANET is to design the robust security.
- Exhaust the victim’s network of resources such as bandwidth and energy (packet delivery ratio) etc.
- Consume the network resources thereby degrading the network performance.

IV. PROPOSED METHOD

Flooding RREQ packets in the whole network will overwhelm a lot of resource of network. To minimize blocking in a network, the AODV protocol adopts some methods. As a part of limitation, a node cannot create more RREQ_RATELIMIT RREQ messages per second. In the Ad Hoc Flooding Attack, the attack nodes violate the above rules to exhaustion the network resource. The attacker tries to send unnecessary RREQ without considering RREQ_RATELIMIT within per second. In the Flooding Attacks, the whole network will be filled of RREQ packets which the aggressor node sends. The communication bandwidth is fatigued by the flooded RREQ packets and the resource of nodes is fatigued at the same moment. For instance, the storage of route table is limited. If mass RREQ packets are transmitted to a node in short duration, the routing table's storage of node will get filled causing node unable to receive new RREQ packets. As a result, the authentic nodes cannot set up routes to send data. In this paper we proposed a new hybrid approach to enhance the performance of MANET in tactical environment as of flooded nodes.

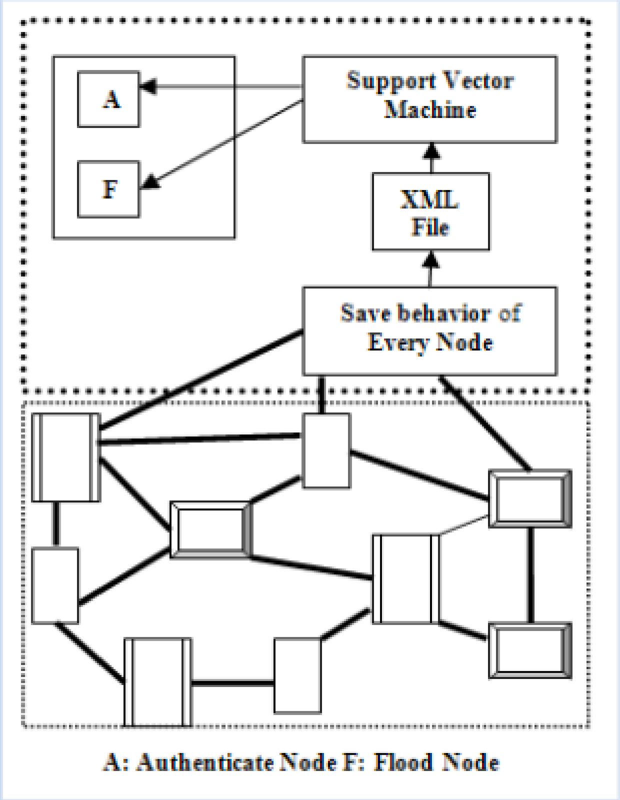

A
F
Support Vector Machine
XML File
Save behavior of Every Node
A: Authenticate Node F: Flood Node

Figure 1: SVM Based Detection Technique

In this method initially collect the behavior of every node then using of this data to find out the flooded malicious node. For this collected behavior of every node pass the support vector machine and check this to threshold limit if the node cross the threshold limit they are detect as a malicious node through the SVM figure 1 shows working of the method.

A. Proposed Solution

In the proposed system we have proposed a new method based on AODV behavioral metrics detect and prevent MANET flooding attacks. In this method we have used the PDER, CO and PMIR as metrics to prediction of flooding attacks. Our proposed method will be implementing on NS-2 test bed. (AODV is a reactive routing protocol and it establishes route on demand).

The essential **SVM** takes a set of input data and predicts, for every given input, which of two feasible classes forms the input. SVM used to classify the node into two groups normal node and malicious (flooded) node.

Advantages of Proposed Method:

1. SVM used to classify the node into two groups normal node and malicious node.
2. We use the PDER, CO and PMIR as metrics to prediction of flooding attacks.
3. Robust security.
4. Good network lifetime (Throughput).

B. Algorithm

```
Proposed Algorithm
1. Collect all the metrics using NS-2 test bed and save.
2. Calculate PDR, CO and PMIR
3. if (PDER>0.9) and ((CO >= 70) and (PMIR > =0.3)
4. Node is flooded
5. Else
6. No-operation
```

PDR (Packet Delivery Ratio) : It is the number of delivered data packet to the node. Greater is the value of packet delivery ratio better is the performance of the node.

PDR= (Number of Packet's Transmitted) / (Total Number of Incoming Packets)

Control Overhead: The ratio of the number of routing protocol control packets transmitted to the number of data packets is known as Control overhead.

CO = (Number of Control Packet's Transmitted) / (Total Number of Packets)

PMIR (Packet Misroute Rate): Node sends packet to the wrong destination is called misroute data packet. PMIR ratio is the number of misroute packet is delivered to the transmitted packets.

PMIR= (Number of Packet's Misrouted) / (Total Number of Incoming Packets)

C. Prevention Method

Problem of paper "A Simulation Analysis of Flooding Attack in MANET using NS-3" threshold limit has been changed by the attacker nodes; we will use this technique for prevention. SVM will be installed on some node for detecting malicious node after detection this node broadcast acknowledgement message to all then all nodes update their routing table and delete the entries of malicious node. If the nodes change the threshold limit for this technique it will detect by the other node. In this scheme we define a normal profile of node using its communication behavioral to other nodes (like PDER, CO, PMIR) if any node deviate from their regular profile that means the node is abnormal and further use this prevention mechanism will take to stop such type of activities.

V. Simulation Results

We use NS2 as the simulation platform. We use three parameters PDER, CO and PMIR to evaluate the correctness and efficiency of the behavior scheme.

Overall, the research can be alienated into two phases - Behavior stage and classification stage. In behavior stage collect the behavior of every node through the simulation. After this pass to this behavior into the SVM machine if the node cross the threshold limit they are detect as a flooded node. In this simulation we compare the performance of different sets of nodes. And analyze the affect, the performance of the network due to flooded node. After detection of this node inform every node about this node and block the transmission of this node.

With the help of these performance activities of each node is been observed. On the basis of their behavior and threshold value SVM classify the nodes. If any of the nodes cross the threshold limit that means it is flooding. As soon as this flooding behavior of the node is detected, all the other nodes are acknowledged about this so that they stop responding to that misbehaving node.

VI. Conclusion

The previous work applies this method for detection of malicious node. In this paper we have discuss a Flooding attack and there affect of the network. Flooding is another type of attack launched using routing request. In this paper we have proposed a solution for finding and prevention of Flooding attacks. Our method is easy and fast. In future this technique will be used to implement to detect other type of attacks

References

[1] Abedellatif Mohammed Hussein, "Flooding Control in Route Discovery for Reactive Routing in Mobile Ad Hoc Networks", Kate Gleason College of Engineering Rochester Institute of Technology Rochester,NY May, 2007.

[2] Luis GironÃ©s Quesada, "A Routing Protocol for MANETs", Norwegian University of Science and Technology, May 2007.

[3] Humaira Ehsan and Farrukh Aslam Khan, "Malicious AODV Implementation and Security and Privacy in Computing and Communications, IEEE, 2012

[4] Ms. Arpita Raverkar, "Route Discovery in Insecure Mobile Ad hoc Network", IEEE, 2011 978-1-4244-8679-3/11

[5] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury "A Simulation Analysis of Flooding Attack in MANET using NS-3", Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Syst,, Feb. 28 2011-March 3 2011.

[6] Casimir & Roland, "The Performance Of Dynamic Source Routing Protocol For Mobile Ad Hoc Networks", Blekinge Institute of Technology September 2009.

[7] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey", The 17 th White House Papers Graduate Research 2004 CiteSeer.

[8] Deepa.S and Dr. D.M Kadhar Nawaz," A Study on the Behavior of MANET Routing Protocols with Varying Densities and Dynamic Mobility Patterns" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[9] Yoav Sasson, David Cavin, and Andre Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks" CiteSeer Conference 2002.

[10] S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam,"A Review on Attack Prevention Methods in MANET" Journal of Modern Mathematics and Statistics Year: 2011