ISSN:0975-9646

Evaluation and Mitigation of DoS attack using behavior Anomaly Detection approach using NS-3

Simmi Jain, Prof.Hitesh Gupta

Computer Science & Engineering
Patel Institute of Sc. & Tech.
Bhopal, India

***Abstract*— Everything has two sides, pros and cons. Mobile adhoc offers instant solution for communication when requires without establishing infrastructure with wireless mobility feature. MANET is a kind of automatic networks which composed of flexible, dynamic, and fully autonomous network entities that can (re)systematize in accordance with the operational, cost-effective, and societal needs of the users and organizations [1]. Although MANET offers quick and fast communication environment using atomicity (multihop routing), its application and performance would be spectacularly obstruct in absence of security measure [1]. One of them attack is Denial of Service attack (flooding) launched via taking the advantages of MANET routing concept (flooding in route discovery) and multihop communication [3] [4]. In this article we have presented a novel approach to detect and prevent flooding (control and data) attack using behavioral anomaly detection technique. The good thing about proposed method is their behavioral classifications that distinguishes normal and abnormal behavior of nodes in MANET and raise the alerts if any deviation detected. The foundation of behavioral profile is inspired from human natures in society like if we want to check, how much a person is cooperative or selfish we will see the exchange of things via particular humans same thing also true in case of MANET i.e PDR (packet delivery ratio).**

Proposed scheme is the extension of our previous work [3] [4] that present the survey on flooding and its impact and second one discusses about the effectiveness of or proposed scheme in DSR routing protocol. In this article we are going to evaluate our scheme in two popular routing protocols of MANET i.e. OLSR and DSR presents the results and discussion about proposed scheme effectiveness. Results show that the performance of proposed method is better than other existing method. Future work of the proposed method will focus on enhancing it capability to apply on WiMax and 4G communication system to detect other types of attack as well and we will also plan it to test it on other routing protocols. Proposed approach has been tested under NS-3.14 MATLAB tools.

Keywords- CO, DoS, DDoS, DSR, Flooding, HELLO, MANET, OLSR, PDR, packet misrouted, NS-3, SVM.

I. INTRODUCTION

Everything has two sides, pros and cons. Mobile adhoc offers instant solution for communication when requires without establishing infrastructure with wireless mobility feature. MANET is a kind of automatic networks which composed of flexible, dynamic, and fully autonomous network entities that can (re)systematize in accordance with the operational, cost-effective, and societal needs of the users and organizations [1].

Although MANET offers quick and fast communication environment using atomicity (multihop routing), its application and performance would be spectacularly obstruct in absence of security measure [1]. One of them attack is Denial of Service attack (flooding) launched via taking the advantages of MANET routing concept (flooding in route discovery) and multihop communication [3] [4].

Although there are lots of convention security approach used in wired network to detect and prevent DoS attack but the main problem with such approach is dynamic nature of MANET because network topology constantly changes. Hence traditional methods are inefficient [2]. Another problem is novelty in attacks (intrusion) hence signature based mechanism does not perform well in such scenario.

In this article we have presented a novel approach to detect and prevent flooding (control and data) attack using behavioral anomaly detection technique. The good thing about proposed method is their behavioral classifications that distinguishes normal and abnormal behavior of nodes in MANET and raise the alerts if any deviation detected. The foundation of behavioral profile is inspired from human natures in society like if we want to check, how much a person is cooperative or selfish we will see the exchange of things via particular humans same thing also true in case of MANET i.e PDR (packet delivery ratio).

Proposed scheme is the extension of our previous work [3] [4] that present the survey on flooding and its impact and second one discusses about the effectiveness of or proposed scheme in DSR routing protocol. In this article we are going to evaluate our scheme in two popular routing protocols of MANET i.e. OLSR and DSR presents the results and discussion about proposed scheme effectiveness.

Rest of the paper is organize as follow section 2 discuss the vulnerabilities in OLSR and DSR routing protocol used by attacker to exploit DoS attack, section 3 insight into our proposed work to detect flooding attack by applying the concept of behavioral based anomaly detection mechanism using NS-3 and SVM, section 4 describes about the simulation and results obtained by using proposed method then finally section 5 concludes the paper.

II. Vulnerabitiies In Dsr And Olsr For Dos Attack

A. DSR

Dynamic Source Routing (DSR) is a main legislature of the on-demand routing protocols of based on the source routing mechanism. In Source routing the transmission of routing information is initiated and supplied by the source node. Then packet transmission takes place from source to the destination [4].

The vulnerabilities in DSR is relies on its working during route discovery that makes it attacker choice to take advantages –

Dynamic source routing (DSR) [5] protocol, is a type of reactive routine methods based on source routing paradigm i.e. originator node knows the complete hop-by-hop route to reach destination. This feature makes it efficient over other but its resultant is overhead of routing messages. Updating the route cache of each node and requesting a route are the building block for flooding (Denial of Service) attack [6].

For more details interested author may refer [3] [4].

Denial of Service Attack in DSR: Author [7] has demonstrated how DSR will be use as a weapon for malicious node for exploiting of DoS attack.

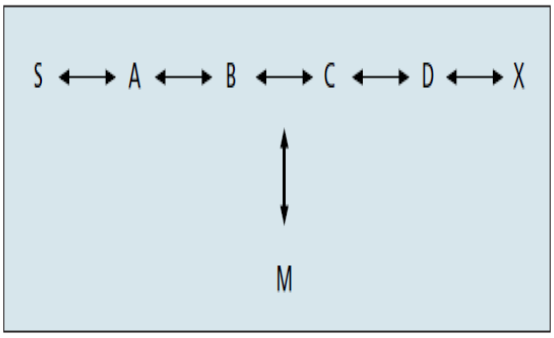

Fig. 1. MANET Topology presented at [7]

As shown in figure 1. DSR [8] utilizes the source routing strategy, thereby source nodes explicitly state routes in data packets. These routes lack any integrity checks, so alterations of source routes in packet headers can be easily performed by malicious nodes, resulting in denial-of-service attacks. Assume a path exists from S to X as shown in Fig. 1. Also assume that C and X are out of the power range of each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S wishes to communicate with X to which it has an unexpired route in its route cache. S transmits a data packet toward X with the source route (S, A, B, M, C, D, X) attached to the packet's header. When M receives the packet, it can alter the source route in the packet's header, e.g. it can delete D from the source route. Consequently, when C receives the altered packet, it attempts to forward it to X. Since X is out of C's power range, the packet will not reach X.

C will then consider that the link with X has been broken, and will send a RER packet back to S via M. When M receives this packet, it will simply drop it. Therefore, S will still use the route through M, and this latter will continue performing this way, resulting in a denial-of-service attack against the routing service. This attack can also be used to cause sleep deprivation, since packets will be transmitted and retransmitted through compromised routes.

B. OLSR

OLSR is a type of table driven routing protocol (proactive). OLSR is a most popular protocol in this category of MANET routing, it maintains the list of available route from all nodes and updates periodically [9]. The core concept of OLSR is MPR (multi point relay) which is special types of node (determined by OLSR during route discovery) which is reachable from all 2-hop nodes in MANET then it sends HELLO message and TC (TOPOLOGY CONTROL) [9][10] [11]-

- First HELLO message is broadcast PERODIOICALLY by all the nodes to all other nodes which include following information o it-
    - Senders address
    - List of neighbors from which control traffic has been heard.
    - List of neighbors with which bi-directionality has already confirmed.
    - List of MPR set of originator node.

HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. HELLO message is used for neighbor sensing and also for selection of MPRs nodes.

- TC messages are also emitted periodically by MPR nodes. TC message contains the list of the sender's MPR selector set. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network. This message is used for route calculation.

The OLSR operation can be summarized as follows:

- Neighbor sensing: To achieve that each node broadcasts to its 1-hop neighbors HELLO messages periodically.
- MPR selection : There are two types of sets
    - MPR set this set of selected neighbor nodes for each node from its 1-hop neighbors. When a node sends a routing message, only the nodes that are in its MPR set forward this message.
    - MPR selector set. Each node also maintains information about the set of neighbors that selected it as MPR which is called MPR selector set.
- Topology Diffusion: Nodes that were selected as MPR must send TC messages to construct routing table. TC messages are flooded in the network and only MPRs are allowed to forward TC messages. Each node in OLSR protocol has two tasks:
    - Correctly generate the routing protocol control traffic
    - Correctly relay the routing protocol control traffic on behalf of other nodes.

Flooding (DoS) in OLSR will be exploited using HELLO and TC messages during finding of MPR and by MPR itself.

III. Proposed Method

This section of article discusses the behavioral based anomaly detection methods of IDS to detect and prevent flooding disruption attack in OLSR and DSR routing protocols using NS-3 test bed.

Before presenting a proposed approach first we will briefly describes what is a an anomaly detection. Intrusion is a unauthorized act to compromise with authorization, confidentiality and availability. IDS is a method of detecting and suspicious or malicious (intrusion) activity in the host or network by applying signature or anomaly detection method. In signature based approach it compares present behavior with known attack signatures and if found it raises the alert. While in case of anomaly detection the system checks the deviation of current profile (behavior) with the normal profile if there is any deviation it will generate alert for announcing the activity to be suspicious in the system. The good thing about anomaly is that it can able to detect unknown (new) attacks because it does not use signature or pattern to match the attacks.

Anomaly based detection is best suited for MANET due to dynamic topologies and nature.

In this paper we have presents a novel approach called behavioral based anomaly detection technique for identifying flooded node (DoS attacker). As our previous research article [3] [4] describe about the behavior metrics used in proposed approach are PDR, CO and PMIR in case of DSR routing protocols and PDR, CO, and number of HELLO messages in case of OLSR flooding identification.

The method of detecting DoS in DSR is already presented in [4] interested author will refer it.

Proposed Method – Proposed method is based on the behavior classification of nodes to detect and prevent flooding attacks in MANET. For this we will use following metrics for behavior rating -

1. **PDR (Packet Delivery Ratio)-**

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

2. **CO (Control Overhead)-** it is measure of total number of routing packets send by a node

3. **PMIR(Packet Misroute Rate)-**

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

4. No_HELLO_msg

It counts the number of Hello Messages of each node

Proposed System Design:

Proposed system work as follow:

1. Collect statistics about node in normal opratin of DSR and OLSR
2. Collect the behavioral metrics (PDR, CO, PMIR, and No_Hello_msg)
3. Make base profile (normal profile)/ behavior
4. Repeat steps 1-3 for each topology and node in MANET
5. Compare behavioral metrics using SVM machine
6. Check the deviation
7. If yes raise the alert and broadcast the message to all with node id cause flooding.

The proposed method provides a cost effective solution for DoS attack. The best thing about proposed approach is their distributed natures that combat against DoS attack quickly and efficiently.

The proposed system has been implementing using modern network simulator NS-3.14 [13] on Ubuntu 12.10 system.

IV. Simulation And Results

Working

The proposed approach provides easy and quick solution for defending against flooding attack. The routing protocol we has been selected for mitigation is DSR because it also uses the flooding mechanism for searching of routes dynamically that's makes it vulnerable for such kind of attack.

Propose solution has two important unit: first, gathering nodes behavior information like packet delivery ratio, control overhead (no of RREQ) and packet misrouted ratio. All such behavior has been stored in a file; different types of mechanism will be used for capturing all nodes statistics like ***.pcap, ASCII . CSV*** or ***xml format.***

Second unit is to reputed the nodes behavior i.e. to identify that whether node is authenticate or suspicious (intruder), for achieving proposed method adopted the idea of linear classification by applying SVM on that behavior, that tells about normality or abnormality of the node.

For developing (simulating) unit one, simulator will be the right test bed for this we have been used modern network simulator NS-3.14 on Ubuntu machine.

Second unit i.e. classifier has been implemented in MATLAB.

Results

1. **Simulation snapshot**

   Figure 2 (a) and (b) shows the simulation snapshot under flooding mitigation using NS-3.14 under Ubuntu 12.10.

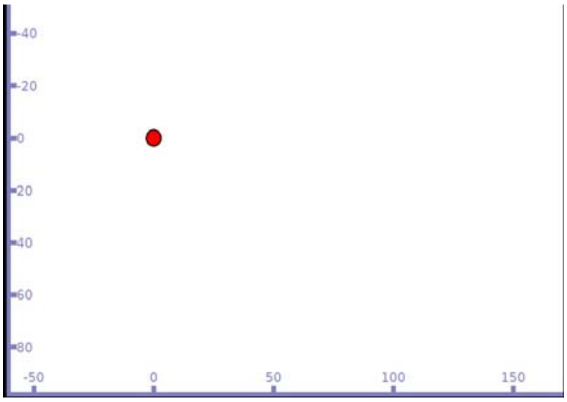

Fig. 2 (a) DSR simulation at time zero

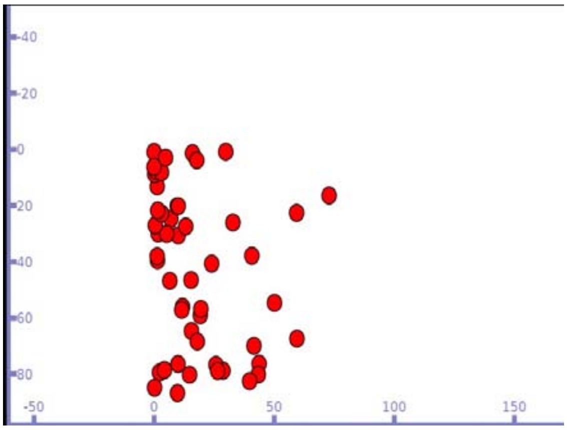

Fig. 2 (b) DSR simulation with 50 nodes

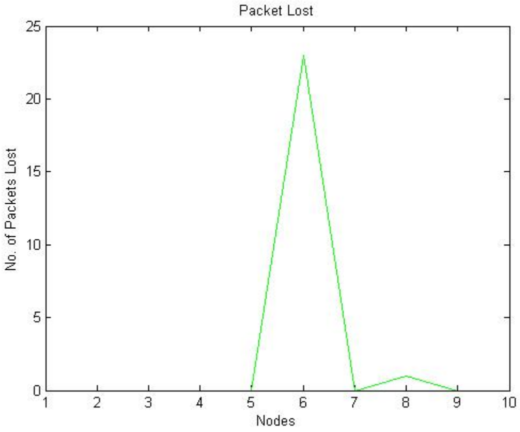

Fig. 2 (c) Packet lost in OLSR in presence of flooded node

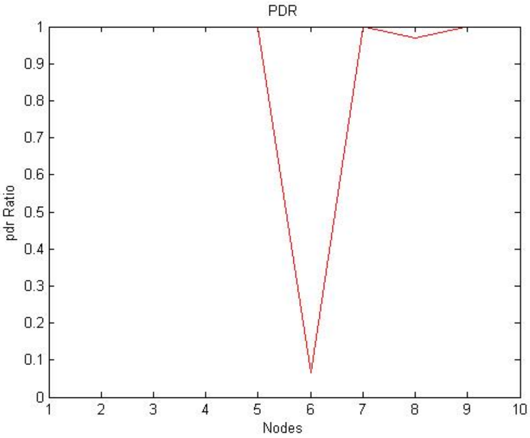

Fig. 2 (d) PDR of OLSR in presence of flooded node

2. SVM OUTPUT

Figure 3 shows the output of SVM classifier that classifies the flooded and authenticated node (non flooding node) based the behavior.

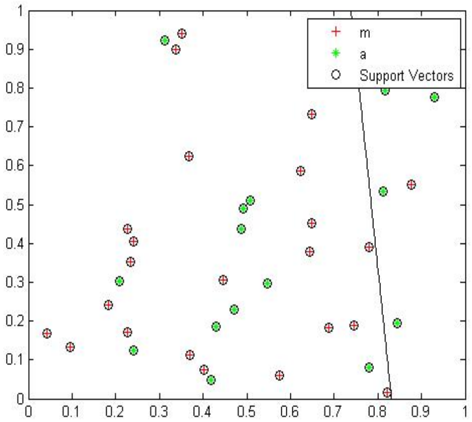

Fig. 3. SVM Classifier output for flooded between authenticate node in DSR

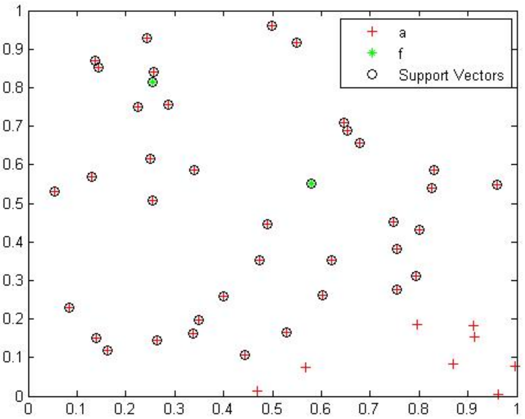

Fig. 3. SVM Classifier output for flooded between authenticate node in OLSR in 50 nodes

V. CONCLUSION AND FUTURE WORK

This article presents a novel anomaly detection scheme to fight against DoS or flooding attack in OLSR and DSR routing protocols in MANET. The good thing about proposed work is its behavioral anomaly detection which is capable of detecting all new types of flooding disruption method will be imposed in MANET. For evaluation the scheme we have choose both types of popular routing protocol hybrid approach to detect and prevent flooding in MANET can be launched via nay proactive or reactive scheme. DSR routing protocol based on behavior reputation. The proposed method is provides the simple and easy to implement mechanism to control suspicious flooding attack in MANET. The anomaly detection mechanism makes it better and cost effective to fight against unknown flooding to be imposed in MANET. For performance and evaluation the ns-3 test bed has been used which produce more accurate results using modern communication parameters. Anomaly detection engine uses the behavior of the nodes to check deviation that’s why it also called behavioral anomaly detection mechanism. Results show that the performance of proposed method is better than other existing method. Future work of the proposed method will focus on enhancing it capability to apply on WiMax and 4G communication system to detect other types of attack as well and we will also plan it to test it on other routing protocols. Proposed approach has been tested under NS-3.14 MATLAB tools.

REFERENCES

[1]. Zonghua Zhang, Farid Naı¨t Abdesselam , Pin-Han Ho and Youki Kadobayashi "Toward cost-sensitive self-optimizing anomaly detection and response in autonomic networks", Elsevier, computers & security 30 (2011) 525-537.

[2]. Meysam Alikhany and Mahdi Abadi "A Dynamic Clustering-based Approach for Anomaly Detection in AODV-based MANETs", IEEE, International Symposium on Computer Networks and Distributed System (CNDS), Feb 23-24, 2011.

[3]. Simmi jain, Hitesh gupta "Detection and prevention of Flooding in MANET using behavioral rating " ***International Journal of Computer Science and Information Engineering (IJCSIE) ,March 2013***

[4]. Simmi jain, Hitesh gupta "Impact and Mitigation of Flooding Attack in DSR using NS-3" , International Journal of Innovation and Applied Studies (IJIAS) , 13-090-08

[5]. Dong-Ii Zhang, Wen-cheng Jiao and Jian-ling Zheng "Research and Improvement of Dsr Protocol in Ad Hoc Network", IEEE, 2nd International Conference on Industrial and Information Systems, pp. 242-244, 2012

[6]. Shams Qazi, Raad Raad, Yi Mu and Willy Susilo "Securing DSR against wormhole attacks in multirate ad hoc networks", Elsevier, Journal of Network and Computer Applications 36 (2013) 582–592.

[7]. DJAMEL DJENOURI, YES KHELLADI and ALGIERS NADJIB BADACHE "A SURVEY OF SECURITY ISSUES IN MOBILE AD HOC AND SENSOR NETWORKS", IEEE Communications Survey, Fourth Quarter, Vol. 7 No. 4, 2005.

[8]. B. David and A. David, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Chapter 5, pp. 153–81, 1996.

[9]. Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, and Ali H. Afsari "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", Elsevier Procedia Computer Science, World Conference on Information Technology, pp. 115-121, 2011.

[10]. Clausen T., Jacquet P., Laouati A., Minet P., Muhltahler P., Qayyum A., and Viennot L., "Optimized Link State Routing Protocol", IETF RFC 3626, 2003.

[11]. OLSR Protocol, available at http://www.olsr.org