INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)
ISSN 2278 – 7631 (Print)

Performance Analysis of AODV Routing Protocol under the Different Attacks Through The Use Of OPNET Simulator

Nidhi Saxena
Institute Of Engineering and Science, Indore, Bhopal, India
Sanjeev Kumar
Netlink Software, Bhopal, India
Vipul Saxena
Oriental Institute of Science &Technology IPS Academy Indore, Bhopal, India

Abstract:
Security is always an important issue especially for the case of Mobile Ad Hoc Network (MANET) because the structure of the network makes it easier target for attackers. It can also be observed that the each type of attack affects the network characteristics differently hence a careful observation & analysis of network characteristics could describe the state of the network such as network is under specific attack or operating normally. Our work is performed in two parts in first part we simulated the network model under different attack using network simulator and during simulation we collected the network characteristics data such as packet drop rate, average number of hops per route, maximum end to end delay etc.. In the second part of our work the collected data is used for training of PNN which finally used for attack classification or detection. The simulation results shows that by selecting effective characteristics and proper training the detection rate up to 90% is achievable.

Key words: *MANET, PNN, Intrusion Detection System*

1. Introduction

The Mobile Ad Hoc Network (MANET) is designed for easier establishment on network without any infrastructure but making design like this also exposed it to network attackers and makes it a soft target for intruder hence extra care is required to be taken. Now to overcome these problems many techniques are proposed one most common is the modification in the protocol (since initially it is designed by considering the performance). Generally the modification in the protocol works for specific attacks only and it may affect the performance also. Another problem with protocol modification is all nodes operating in that network must have same protocol or modifications must be compatible with standard one. Another approach which can work independently on any specific node or even on a separate observer unit is generally known as Intrusion Detection System (IDS). An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Although the IDS do not counter the attack but it can generate alarm. The analysis shows that both systems have their own limitations but a better system can be designed by combining the both algorithms the IDS system can used to initiates the specific modification in protocol and this could be the complete solution for the intrusion detection and prevention system (IDPS).

2. Related Work

Because of the importance of the subject already some work has been done some of them which are found most related and useful for making this paper is presented here. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei [1] presented great literature on the MANET attacks. Their work gives the detailed explanation of different attacks their behavior and their effect on network characteristics they also explained the security mechanism for some attacks although no simulation and mathematical details are provided. Another text on same topic is presented by Abhay Kumar Raiet.al. [2]. the simulation and modeling of the different attacks on MANET using network simulator is explained in [3] the paper also discussed the protocols and their immunities to different attacks with analytical modeling and mathematical formulation. Farah Jemili et.al. [4] Presented the intrusion detection system based on Bayesian Network (BN). The BN is used to build automatic intrusion detection system based on signature recognition. The goal is to recognize signatures of known attacks, match the observed behavior with those known signatures, and signal intrusion when there is a match. Improved Support Vector Machine(SVM) based IDS model is presented in [5]the paper discussed the method for improvement of SVM to achieve the

higher accuracy. A data pre processing and removal of similar data to reduce the training data size using k means clustering presented in [6] which shows significant improvement in training time with maintaining accuracy. One important requirement of classification is parameter selection because some of the features may be redundant or with a little contribution to the detection process. Gholam Reza Zargar and PeymanKabiri [7] investigate selection of effective network parameters for detecting network intrusions. The study shows that the major difficulty in develop the system like presented in [5][6][7] is that intrusions signatures changes broadly hence a large training dataset, parameter selection, data filtering and optimal classification is required. Besides mentioned limitation it has a great advantage of better classification without affecting the network performance.

3. Routing Protocol

Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV. This research paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The objective is to make observations about how the performance of these protocols can be improved. There is various type of routing protocol.
These are following AODV, OLSR, DSR, and ZRP. [11].

3.1. AODV Routing Protocol

It provide fast efficient route establishment between mobile nodes that need to communicate with each other. Since AODV has been specifically designed for Ad Hoc wireless network. In addition to unicast routing, AODV support multicast and broadcast as well. AODV can be extended to support Quality of Services (QoS). AODV is an on demand algorithm, which means that routes between nodes are built only when means they are requested by originator nodes. Routes are maintained only as long as originator need then.

3.2. OLSR Routing Protocol

This protocol is based on link state algorithm and it is proactive (or table- driven) in nature. It employs periodic exchange of message to maintain topology information of the network at each node. OLSR is an optimization over a pure link state protocol as it compact the size of information sent in the message and furthermore reduces the number of retransmission to flood these messages in entire network. This protocol uses the multipoint broadcasting (relaying) tech to efficient and economically flood its control message.

3.3. DSR Routing Protocol

DSR routing protocol, which are used fir efficient routing under different scenario in MANET, which play a critical role in place where wired network are neither available nor economical to deploy. DSR allows the network to be complete self organization and self configure, without the need for any existing network infrastructure or administration. The protocol composed of two mechanism of route discovery and route maintain which work together to allow nodes to discover and maintain source route to arbitrary in the ad hoc network.[13]

3.4. ZRP Routing Protocol

ZRP is a well known hybrid routing protocol that is most suitable for large scale network. The ZRP framework is designed to provide a balance between the contrasting proactive and reactive routing approaches. its name is derived from the use of one that define the transmission radius for every participating node ZRP uses a proactive mechanism of node discovery within a node's immediate neighborhood, while inter zone communication is carried out by using reactive approaches.[12]

4. Descriptions of MANET Attacks Analyzed In This Study

There are different type of attacks may depends upon specific routing protocol or on specific requirement of attacker. In this section we are only presenting a brief explanation of the attacks used for testing of proposed work.

4.1. Black hole Attack

The this attack, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Then the attacker consumes the intercepted packets without any forwarding.

4.2. Wormhole Attack

In this attack the attacker records packets at one location in the network and tunnels them to another location and during the tunneling it can also read and temper the packets. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole [8].The attack could prevent the discovery of any routes other than through the wormhole.

4.3. Selfish Attack

Nodes that do not forward other's packets, thus maximizing their benefit at the expense of all others. They are assumed to always behave rationally, so they cheat only if it gives them an advantage.

4.4. Sleep Deprivation

Consists to make a node to remain in a state of activity and to make him consume all its energy. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

5. Probabilistic Neural Network (PNN)

In a PNN, the operations are organized into a multilayered feed forward network with four layers.

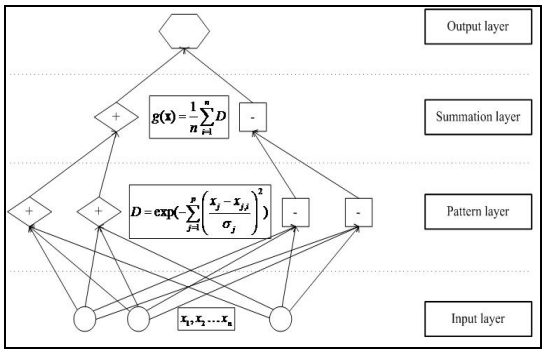

Figure 1: Structure of PNN [10]

The input nodes are the set of measurements. The second layer consists of the Gaussian functions formed using the given set of data points as centers. The third layer performs an average operation of the outputs from the second layer for each class. The fourth layer performs a vote, selecting the largest value. The associated class label is then determined [9].

6. Proposed Algorithm

In the proposed system we firstly simulate the different attacks on the MANET using network simulator and obtain the different parameters (table 1) during simulation. Now after collecting all the parameters a neural network is trained this is later used for classification of attack. The algorithm can be described in detail by following steps:

- Step 1: Design a MANET in network Simulator of selected configurations (table 2).
- Step 2: Configure different scenarios for different attacks (table 3).
- Step 3: Simulate all the scenarios and collect the parameters (table 1).
- Step 4: Formulate the table by sampling the collected data at specific intervals.
- Step 5: Normalize the each parameter by detecting its maximum and minimum values according to the following formula

  $$V_{norm} = \frac{V - V_{min}}{V_{max} - V_{min}}$$

  $Where:$
  $V = Designatestheactualvalueof$
  $parameter.$
  $V_{min} = Designatestheminimumvalueof$
  $parameterfromallsenarios.$
  $V_{max} = Designatesthemaximumvalueof$
  $parameterfromallsenarios.$
  $V_{norm} = Designatesthenormalizedvalue$
  $ofparameterfromallsenarios.$
- Step 6: The normalized values set are arranged in an array to represent system condition by a vector this vector can be represented by

  $$Trn_{vect} = [V_{norm1}, V_{norm2}, V_{norm3}, \ldots\ldots V_{normn}]$$

  Hence the system states can be treated as n dimension vector.
- Step 7: Group all Trn_{vect} according to attack scenario they represents.
- Step 8: Now these vectors with their classification group are used to train the Probabilistic Neural Network (PNN).
- Step 9: Ones PNN got trained it can now be used as an attack detector.

- Step 10: Now for estimating the threat at any time we can sample the network characteristics at any time and apply (after normalizing) it to the trained PNN.

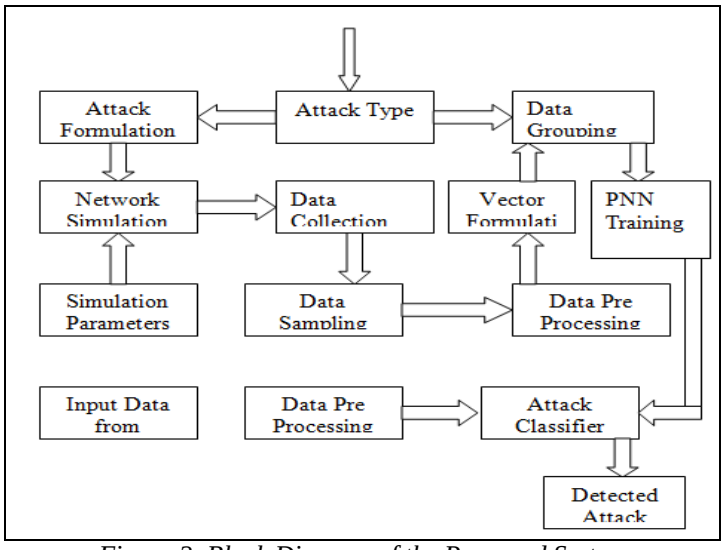

Figure 2: Block Diagram of the Proposed System

7. Simulation Results

The results from simulation of the different attack model in network simulator are shown in while the other details are shown in table 1, 2 and 3. The classification part of the proposed work is performed using MATLAB 7.5 Neural network toolbox in IBM P4 dual core 2.4 GHz processor with 2 GB of RAM and windows XP operating system. The results from this simulation are shows in tablet 4.1 and 4.2.

Average Number of Hops Per Route
Average Route Discovery Time (in Seconds)
Average Routing Traffic Received (Packet/Sec.)
Average Routing Traffic Sent (Packet/Sec.)
Average Packet Drop
Average Route Error Sent
Average Route Replies Sent
Average Route Request Sent

Table 1: List of Collected Parameters

Parameters Name	**Value**
Number of Nodes	20
Simulation Time	60 Second
Area	1km x 1km
Node Velocity	10 km/h
Packet Size	1024 Bits
Routing Protocol	AODV
Transmitted Power	5mW
Antenna Type	Omni-directional

Table 2: Network Configuration

Attack
Black hole
Wormhole

Table 3: List of Attacks Simulated

	TPR	TNR	FPR	FNR
Normal	1	0.7667	0.0333	0
Black hole	1	0.8	0	0
Wormhole	0.5	0.8	0	0.5

Table 4.1: Performance of Probabilistic Neural Network for Different Attacks

	Accuracy	Precision	Recall	F-measure
Normal	0.9667	0.8571	1	0.9231
Black hole	1	1	1	1
Wormhole	0.9	1	0.5	0.6667

Table 4.2: Performance of Probabilistic Neural Network for Different Attacks.

8. Conclusion

The model of the attack detector for MANET presented in this paper is not only capable of attack situation but can also classifying the individual attacks. The Detection accuracy of the system is up to 90% which is excellent also the algorithm have very low FPR (max 8.3%) hence reduces the chances of false alarming. The results also shows that it takes only 0.0075 seconds to identify the condition hence fast enough to prevent any damage due to delayed action. Further it could achieve much better performance by increasing the number of samples taken and increasing the number of characteristics parameter selected.

9. Acknowledgment

I would like to take the opportunity to thank people who guided and supported me during this process. Without their contributions, this research would not have been possible.

We are thankful to our supervisor YagyapalYadav, our friends who help us during our hard times when we need their assistance during thesis study and simulation. We are especially thankful to our parents and brothers, who had always, gave us the courage, best wishes and support during our career. We also have best regards for IES-IPS Academy Indore faculty including Deepak Chauhan who had been helpful throughout our master degree.

10. References

1. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks”, wireless/mobile network security, 2006 Springer.
2. Abhay Kumar Rai, Rajiv RanjanTewari and Saurabh Kant Upadhyay “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).
3. Dr. Karim KONATE and GAYE Abdourahime “Attacks Analysis in mobile ad hoc networks: Modeling and Simulation”, 2011 Second International Conference on Intelligent Systems, Modeling and Simulation, 2011 IEEE.
4. Farah Jemili, Dr. Montaceur Zaghdoud and Pr. Mohamed Ben Ahmed “A Framework for an Adaptive Intrusion Detection System using Bayesian Network”, 2007 IEEE.
5. Jingbo Yuan , Haixiao Li, Shunli Ding and Limin Cao “Intrusion Detection Model based on Improved Support Vector Machine”, Third International Symposium on Intelligent Information Technology and Security Informatics, 2010 IEEE.
6. Z. Muda, W. Yassin, M.N. SulaimanandN.I.Udzir“Intrusion Detection based on K-Means Clustering and OneR Classification”, 2011 IEEE.
7. http://link.springer.com/chapter/10.1007%2F978-3-642-14400-4_50?LI=true#.
8. Martin Schütte ” Detecting Selfish and Malicious Nodes in Manets”, Seminar: Sicherheit In Selbstorganisierenden Netzen, Hpi/Universität Potsdam, Sommersemester 2006.
9. http://www.personal.reading.ac.uk/~sis01xh/teaching/CY2D2/Pattern3.pdf
10. http://voyagememoirs.com/pharmine/2008/06/22/probabilistic-neural-network-pnn/
11. Current Research Work on Routing Protocols for MANET: A Literature Survey G. Vijaya Kumar 1, Y. Vasudeva Reddyr 2, Dr. M. Nagendra 3 1 CSE Dept, Asst. Prof, G. Pulla Reddy Engg. College (Autonomous), Kurnool-2, AP, India 3 MCA Dept, Asst.Prof, G. Pulla Reddy Engg. College(Autonomous),Kurnool-2,AP,India 3 CS&T Dept, Assoc Prof, SKU, Anantapur, AP, India
12. Nidhisaxena, Yagyapal Yadav, Vipul Saxena Review Report ATTACK Analysis in Mobile Ad HOC Network Based on System Observations International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013
13. Implementing and comparing DSR and DSDV routing protocols for mobile AD Hoc networking”Bikas Rathi”.