ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 1 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Characterization of Framework for Detection & Prevention of DoS Attacks in Wireless Ad Hoc Network

[I]Lokhande S.N., [II]Dr. Khamitkar S.D.
[II]Assistance Professor, School of Computational Sciences, SRTM University, Nanded
[II]Associate Professor, School of Computational Sciences, SRTM University, Nanded

Abstract
As wireless networks is gaining popularity in last few decades. Due to open medium, dynamically changing topology, no central controller Ad Hoc networks are prone to different types of DoS attacks. The most sever and easy to launched attacks are data flooding and black hole DoS attacks in Ad Hoc networks. In this paper we studied the effect of DoS attack on Ad Hoc networks performance. We also propose a framework which is able to detect and prevent the Ad Hoc network from data flooding and black hole. Our proposed framework works on the basis of monitoring the network parameters for detection and identification of attacks.

Keywords
Ad Hoc networks, DoS attacks, IDS, NS-2, Otcl.

I. Introduction

The various attacks against mobile nodes are flooding, black hole, warm hole, packet dropping and Byzantine attack etc. It is important to search new architecture and mechanisms to protect the wireless networks and mobile computing application. Intrusion Detection System (IDS) tools are suitable for identifying these attacks. IDS analyze the network activities by means of audit data and use patterns of well known attacks or normal profile to detect potential attacks. There are two methods to analyze: misuse detection and anomaly detection. Misuse detection is not effective against unknown attacks and therefore, anomaly detection method is used. In this approach, the audit data is collected from each mobile node after simulating the attack and compared with the normal behavior of the system. If there is any deviation from normal behavior then the event is considered as an attack. This research paper focuses on two different DoS attack model i.e. data flooding and black hole scenarios.

II. Basic of Our IDS:

It is a Statistical Based Intrusion Detection system which is based on the principle that intrusions can be detected by inspecting a system's audit trail data for anomaly, and that the audit trail data is noticeably different when an intrusion occurs.
To detect any unusual activity, SBID systems require a depiction of system activity that is considered "normal". Any sequence of system events deviating from the "normal" profile by a statistically significant amount is flagged as an intrusion attempt [1].
Based on this, in our framework, we identify network parameters which are affected during attacks, and characterize their values when the system is normal without any attack.
Our idea is that, by identifying and monitoring network parameters that are affected by various types of attacks, we could measure the relative change in these parameters values from the "normal" values and detect an attack. Once an attack is detected, proper level of protection measures could be applied and hence, nodes causing these attacks could be blocked from accessing the system or the network.

III. Attack Models

To support our base of using network parameters to detect and respond to intrusion, we select two different DoS attack scenarios in Ad Hoc network and their effect on the network parameters.
1] Data Flooding DoS attack: In a type of DoS attack, an intruder bombards packets on a host node which is servicing multiple mobile nodes. In this attack, the attacker creates huge traffic in the link between the attacker and the host resulting in the rapid exhaustion of the networks hosts' precious resources. This kind of DoS attack results in the inability of the host node to serve the other genuine nodes in network fairly.

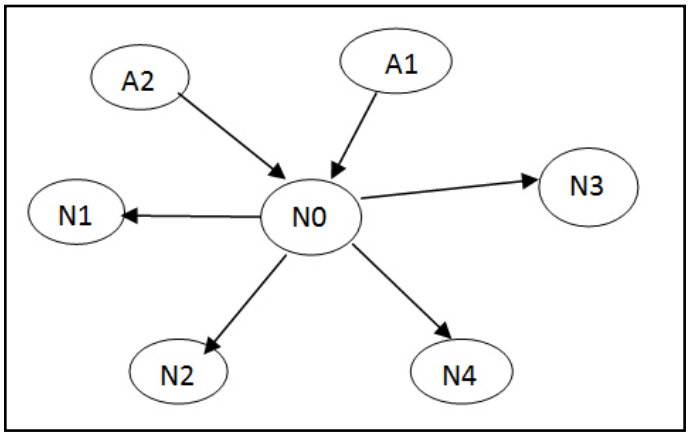

Fig. 1: Data Flooding Attack

Data flooding DoS attack is depicted in Figure 1 where node N0 is a host node and A1 and A2 are the Attackers. The attacker nodes A1 and A2 create a huge traffic resulting in the exhaustion of the node N0's resources. This results in the inability of node N0 to serve genuine nodes N1, N2, N3 and N4 fairly. Some of the critical parameters that are affected by this type of DoS attacks are:
Packet Drop: Due to DoS attacks, packets in the link may be dropped due to exhaustion of the hosts' resources.
Queue Length: The inability of the host to service the request from other nodes because of DoS attacks results in increase in queue length on the links between the host and other nodes.
Energy consumption: The bombardment of packets due to traffic and servicing them result in the consumption of significant battery power in the link between attackers and host.
2] Black Hole Attack: In a black hole attack a malicious node send a forged RRep to source, that it has a fresh and short route towards the destination. When a link is established then the malicious node simply does not perform its intended function of forwarding the packet to a proper destination node and routes all packets to it and later discards/drop them.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

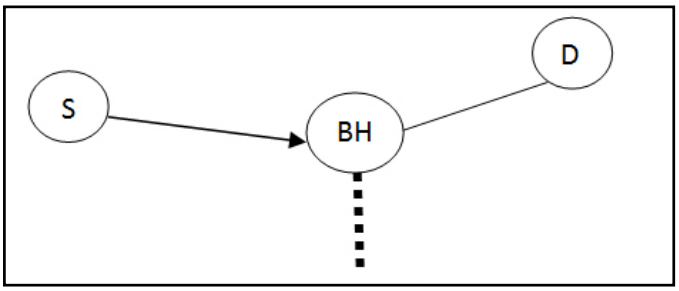

Fig. 2: Black hole Attack

As shown in Figure 2, the packets are supposed to traverse from source node S to destination node D. However, the black hole node BH attracts and discards/drop the packets from S and hence the packets from S never reach D. This results in 'black hole' attacks. Due to this a genuine nodes are unable to access the intended services. Some of the critical parameters that are affected by this kind of attack are:

Throughput: Due to packet mistreatment by selfish nodes, packets do not generally reach host nodes. This results in packet loss, and hence a significant decrease in the measurement of throughput for the destination hosts nodes.

Packet drop rate: Packets are discarded by selfish nodes and hence there is a significant increase in the packet drop rate for the collaborating selfish nodes in ad hoc network.

IV. Related Work

Most of current works on IDS for ad hoc networks employ either distributed or cooperative architecture or distributed and hierarchical architecture.

Zhang and Lee [2] proposed the first distributed and cooperative anomaly-based IDS framework. In this framework, local anomaly detection engine is built on a rule based classification algorithm. RIPPER and local response is activated when a node locally detects an anomaly or intrusion with high confidence. When a node detects an anomaly or intrusion with weak evidence, it then initiates a global intrusion detection procedure through a cooperative detection engine.

Yu Liu and Yang Li [3] node-based anomaly IDS for ad hoc networks using cross-feature analysis technique. It uses the MAC layer feature set to characterize normal behavior of mobile nodes. They have illustrated how feature vectors are constructed from audit data, and how to perform cross feature analysis on these feature vectors.

Chi Hoon Lee et al. [4] proposed another approach using Genetic algorithm combined with selective naïve Bayesian classifiers (SNBN). They used GA for feature selection and SNBN for evaluation. Their experiments result shows that the performance of GA is impressive, compared to IDS with all features while detecting unknown attacks.

Srilatha Chebrolu et al. [5] used two data mining techniques namely Markov blanket feature selection and Classification and Regression Trees (CART) for feature selection and classification in intrusion detection system. Therefore, the above two techniques were combined to create ensemble approach. Finally, they proposed a hybrid architecture involving ensemble and base classifiers for intrusion detection based on the performance of detection rate.

The related existing ad hoc network intrusion detection and intrusion response approaches suffer from one or more of the following limitations:

- Lower detection rate when mobility is used as a parameter.
- Higher false positive rate when mobility is used as a parameter.
- Appropriate response techniques to protect MANET after threat detection.

V. Proposed System

Architecture

Our proposed framework is statistical based and cooperative in nature, which detects the intrusion by observing the networks/ nodes audit trial data (log data) for anomaly. Because the audit trial data is differ in the DoS attacked phase. The proposed framework is distributed and cooperative where every node in the wireless ad hoc network participates in intrusion detection and response activity.

Our framework is basically divided in two parts, first part performs the task of detection of flooding and black hole DoS attack and the second part is responsible to perform the corrective measure to prevent the Ad Hoc network from these attacks. Following are the major steps performed by our framework to detect and defend against the DoS attacks in Ad Hoc networks.

Step-I: In this step the raw data from Ad Hoc network is collected and feed to the identification framework. This step preprocesses the log data to make it suitable for intrusion identification.

Step-II: This step identifies the nodes significant parameters, which are used in detection and as well as prevention framework.

Step-III: This step is used to calculate the Upper Limit (UL) and Lower Limit (LL) values in order to differentiate the normal and vulnerable state of the network parameters.

Step-IV: This step finds the threat index value for node from the thresholds of nodes significant parameters. This threat index value is used to detect a node under attack.

Step-V: On the basis of threshold values of nodes significant parameters this step detects a specific type of DoS attack. Then it calls the prevention model to defend against detected and identified DoS attack.

Step-VI: The Response and Prevention framework gets invoked when the Threat Index computed by the detection framework is in the vulnerable state. The response and protection framework identifies the intruder/attacker and responds to the attack with the response action plan.

The response and prevention model when gets execute, performs the corrective measures as per the identified DoS attack in identification model and maintains the networks normal status.

VI. System Implementation

To verify the performance of our proposed model we simulate the model in SN-2[6]. NS-2 is a discrete event simulator and it is widely used network simulator in research and testing. It is based on two languages: an object oriented simulator, written in C++, and an OTcl interpreter, used to execute user's command scripts. NS has a rich library of network and protocol objects.

The various simulation parameters and its corresponding values of NS-2 simulation environment are specified using the Tcl script. Normal profile is collected in the absence of attacks. The attack profile is created by simulating the black hole and flooding attacks. Various traffic related features like packets sent, packets received, packet dropped, packet forwarded, and transmission delay are collected.

The data collected in a file is preprocessed to get appropriate form

used for detection, AWK script is used for preprocessing.
Training data: The attack data is compared with normal profile and labeled. The classification label consists of two classes namely, normal and abnormal. This data set is used to train the model.
Test data: Test data is collected by simulating black hole and flooding attacks by varying the attackers. It will be given as input to the model to identify whether the particular event is an attack or normal.

VII. Performance Evaluation

The effectiveness of the proposed framework in defending against the DoS attack will be evaluated using the performance measurement by the parameters like Detection Rate, False Positive Rate and False Negative Rate. Detection Rate is defined as the ratio of the number of attacks being detected correctly to the total number of attacks occurred. False Positive Rate is defined as the ratio of the number of attack free events falsely being identified as anomalies to the total number of events. False Negative Rate is defined as the ratio of the number of attack events falsely identified as normal events to the total number of events.

VIII. Conclusion

In this paper we studied the effect of two severe DoS attacks black hole and data flooding on Ad Hoc network. We also identified the network parameters which are affected due to these types of DoS attacks in Ad Hoc network. To prevent the Ad Hoc networks from these DoS attacks we proposes the defense framework , which is able to detect an ongoing DoS attack and prevent the system by executing the appropriate action plan.

References

[1] *H. Debar and A. Wespi, "Aggregation and correlation of intrusion detection alerts," in Proceedings of Fourth International Symposium on Recent Advances in Intrusion Detection, 2001, pp. 85-103.*
[2] *Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.*
[3] *Yu Liu, "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", GameNets'06, October14, 2006, Pisa, Italy. ACM 1-59593-507-X/06/10*
[4] *Chi Hoon Lee, Sung Woo Shin and Jin Wook Chung, "Network Intrusion Detection Through Genetic Feature Selection", SNPD, IEEE, 2006.*
[5] *Chebrolu, S., A. Abraham, J. Thomas, Feature deduction and ensemble design of intrusion detection systems, Journal of Computers & Security,vol-24,295-307, 2005.*
[6] *NS-2 : http://www.isi.edu/nsnam/ns*