Improvement and Performance Evaluation of Correlation Based IDS in MANET

Shiman Sardana[1] Sandeep Garg[2]
[2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]RPIIT, Karnal, Haryana -132001, India

Abstract— Security is a prime concern in mobile ad hoc network (MANET) because of its inherent vulnerabilities. The open and dynamic environment of MANET makes it vulnerable to various security attacks. In this research work we have developed a unique correlation based IDS model for detection of DDOS attack in IMANET (Internet based Mobile Ad hoc Networks). The DDOS attack model is based on parameters which include (probe interval, rate, read interval, read length etc) and the detection and response model is based on the concept of opposing correlation in which the historical covariance values selected defines normal and abnormal threshold is compared with current covariance values in an iterative manner which in shows that both strong and weak covariance is also taken into consideration. Pair wise covariance helps IDS to analyze three routing parameters which are essential for evaluating performance of any MANET. These include PDR, PLR, control messages (Hello, ACK, REQ, and REP). Montecarlo simulation model used here gives us real kind of scenarios which help us to give insight and build sub systems. Proposed algorithm is better in terms of being sensitive and more reliable.

Key words: MANET, DDOS attack, EAACK, AODV

I. INTRODUCTION

The mobile wireless networks are classified into two types: Infrastructure and Infrastructure less networks (multi-hop).The infrastructure network are connected through a wired to one the base Station (one computer) to another based station. But in infrastructure less network have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The infrastructureless networks is also known as Mobile ad hoc Networks (MANET).

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infrastructure or centralized administration. In such a network, each mobile node operate not only as a host but also as a router, forwarding packets for other mobile nodes in the network, that may not be within the direct reach wireless transmission range of each other. The idea of an ad hoc network is sometimes also called an infrastructure-less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. Examples of the possible use of ad hoc networks include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting.

A wireless ad hoc network is decentralized types of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure access point in infrastructure wireless network or the routers. The each node in the network are actively participate in the network for forwarding the data to the other nodes and so the determination of which nodes forward data is made dynamically based on the network connectivity

Wireless ad hoc networks can be classified by their application as wireless sensor networks (WSN) and mobile adhoc network (MANET) Devices of MANET network is free to move independently in any direction that's why linking with any other devices is easily done. The primary goal of Mobile ad hoc network is each device to continuously maintain the information required to properly route traffic.

II. RELATED WORK

Sushma Kushwaha [1] implemented the method of Intrusion Detection System, which is based on the principle of network, nodes or information misuse detection system, which can accurately compare the signatures of known attacks and has a low rate of packet dropouts alarms. They bounded wireless mobile ad-hoc network nodes to getting updates from unknown or unwanted nodes on the same network through routing table; using a Novel intrusion detection technique with the help of routing protocols in MANET (mobile ad hoc network). MANET is very popular and efficient, easy and secure way of communication between two or more mobile user ends and we can send and receive data, information, updates and signals from one end to another known end securely by using Novel Intrusion Detection System technique and by blocking unknown nodes in MANET.

Harisha Datla [4] explained Manet doesn't need a set network infrastructure, each single node works as each a sender and a receiver and they trust their neighbours to relay messages. Unfortunately, the open medium and remote distribution of Manet create it at risk of numerous kinds of attacks. So, it is essential to develop efficient intrusion-detection mechanisms to protect MANET from attacks. They defined solid privacy requirements regarding malicious attackers in MANET and implemented a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances while does not greatly affect the network performances

SMadhavi et al. [16] have examined the vulnerabilities of wireless networks and included intrusion detection in the security architecture for mobile computing environment. They have propose an mIDS(Mobile intrusion detection system) suitable for multihop adhoc wireless networks, which detects nodes misbehavior ,anomalies in packet forwarding such as intermediate nodes dropping or delaying packets. mIDS rely on overhearing packet transmissions of neighboring nodes.

Huang et al [18] have proposed an IDS which uses a specification-based technique for attacks that violate the specifications of AODV directly and anomaly-based technique for other kinds of attacks such as DOS.

Martuza Ahmed, Rima Pal: A network based approach to intrusion detection and prevention, IEEE 2009 [19] introduces a system which detects the routing misbehavior in MANET, Commonly routing protocols for MANET are designed based on the assumption that all participating nodes are fully cooperative. Node misbehavior take place, due to the open structure and scarcely available battery based energy. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuses to forward the data packets or delay of packets.

III. RESULT ANALYSIS

In this research work, an average of 5 nodes communicating with each other as been empirically calculated has been considered as one of constant parameter for further analyzing volume of control messages exchanged when it is under adversity or otherwise. This means at any given time, slot no of exchange of discovery messaged which help to establish link between nodes at regular interval maybe closed to average of 10 messages, one for sending(Hello) and one for sending (ACK). Since there are 5 nodes communicating with each other for one particular time slot, average of 10 messages may occur. Value of 10 may drop either in case when distance between 5 communication nodes increases beyond transmission range or explicitly they are no longer communicating with each other(power off) which is considered as normal scenario . However we have also considered variation in calculation of these messages by using the the control limits formula. Therefore we have two ranges upper and lower which represents normal ranges and when correlation with historical values of these statistics are calculated these upper and lower range automatically corresponds to multiple possible scenarios in correlation which include weak and strong correlation which is indication from above after attack exchange of messages lead to erratic behaviour leading to either weak or no correlation showing that there is huge abnormal activity going in the network.

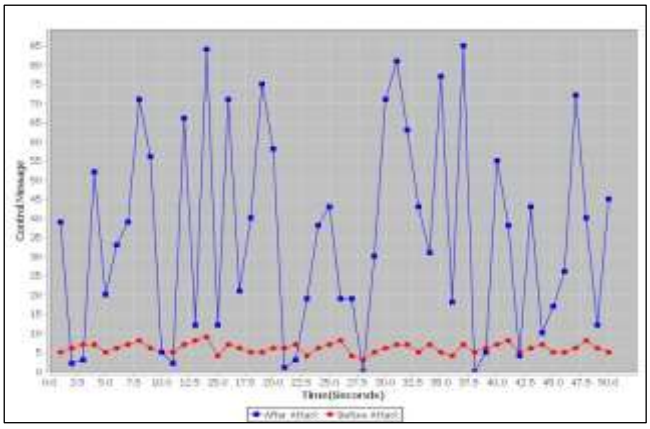

Fig. 1.1: HELLO/ACK Before and After Attack

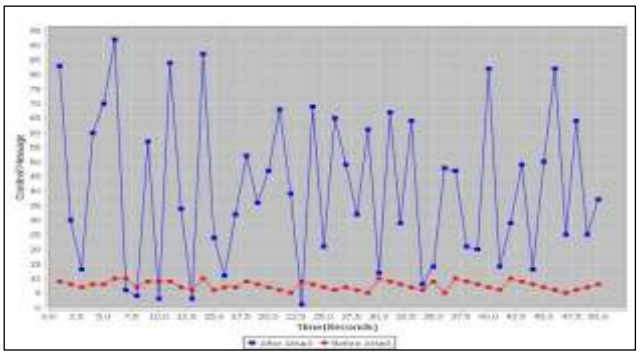

Fig. 1.2: Request/Response Before and After Attack

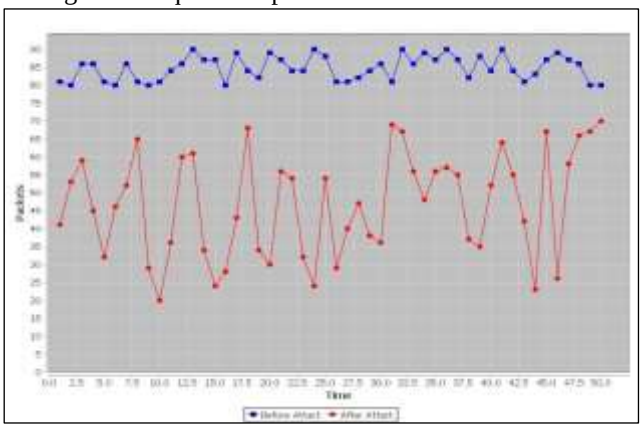

Fig. 1.3: PDR before Attack and After Attack

Typically the shape of traffic if it follows particular distribution for considerable time, PDR would remain in a consistent range as it is not prone to any cystality or any other factor. Since we have developed a simulation which works assuming this consistency, PDR during the normal operation varies between 80 and 90 and there is little variance or standard deviation as such but the moment DDOS attack is introduced the graph becomes unpredictable with the high mortality and erectness in terms of delivering packets to destination. This is attributed due to large UDP based multicast flood of packets which are not letting normal work of services which in fact leads to denial of services.

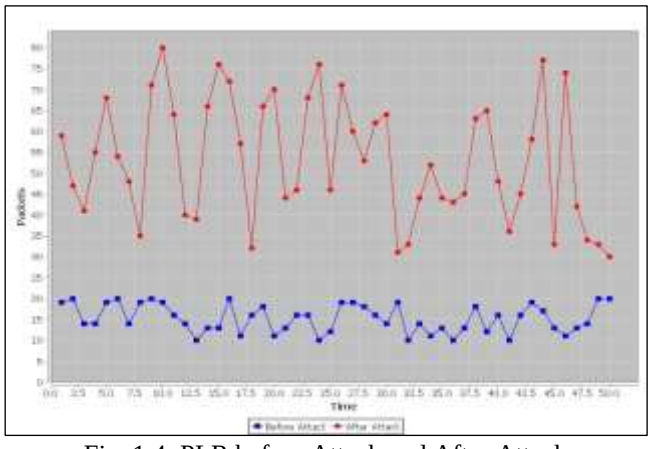

Fig. 1.4: PLR before Attack and After Attack

PLR would remain in a consistent range as it is not prone to any crystallites or any other factor. Since we have developed a simulation which works assuming this consistency, PLR during the normal operation varies between 15 and 20 and there is little variance or standard deviation as such but the moment DDOS attack is introduced the graph

becomes unpredictable with the high mortality and erectness in terms of packets loss to destination.

IV. FUTURE SCOPE

The proposed system can be enhanced in future by other researchers in the following ways:

- In this, only AODV protocol is used, within which there is no method of verification of unsolicited messages and due to periodic beaconing unnecessary bandwidth is consumed. The work can be implemented and analyzed along with other protocols which can help reduce the bandwidth consumption and provides verification of the messages.
- The work is performed only with DDOS attack. The work can be enhanced by implementing some other attack such as black hole, wormhole, authentication etc.

V. CONCLUSION

In this research work it is clear that the correlation concept is producing reliable results in terms of identification of abnormal and normal activity under the scenarios and parameters and methods given in the methodology section, this is because this technique is better than the previous techniques in terms of the following factors: Control limits used which helps the values to find out if there is weak correlation or strong correlation, historical values which are defined helps in setting the limit and then current values are calculated dynamically.

Correlation research provides a good starting position. It allows determining the strength and direction of a relationship so that later studies can narrow the findings down and if possible determine causation experimentally. From the graphs of PDR, PLR there is high impact on the performance of the network; in fact it is clear all mobile nodes are unable to communicate with each other once the attack is introduced. The implementation is performed in java and analysis is presented using a snapshots and graph.

REFERENCES

[1] Sushma Kushwaha, Vijay Lokhande, "Security in Wireless Mobile Ad-Hoc Network Nodes Using Novel Intrusion Detection System", Vol.6,Issue 4, 2016.
[2] K. Spurthy, T. N. Shankar ,S.Sabari Giri Murugan "Enhancement of Intrusion-Detection System in MANETs with the Digital Signature via Elliptic Curve Cryptosystem", Vol. 14, No. 6, June 2016
[3] G. Gowthaman, G. Komarasamy, "A study on secure intrusion detection system in wireless MANETs to increase the performance of Eaack", IEEE, August 2015
[4] Harisha Datla, Mallikarjun Reddy D, Santosh Naidu P, "Performance Evaluation and Testing of EAACK Secure IDS for MANETs", (IJCTT) – volume 17 number 1 – Nov 2014
[5] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. @ 2006 Springer.
[6] Sevil Sen, John Andrew Clark, "Intrusion detection in mobile ad hoc networks", Guide to wireless ad hoc networks,pp.427-454 @ 2009 Springer.
[7] Uppuluri P, Sekar R (2001) Experiences with Specification-based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189.
[8] Tseng C-Y, Balasubramayan P et al (2003) A Specification-Based Intrusion Detection System for AODV. In Proc of the ACM Workshop on Secur in Ad Hoc and Sens Net (SASN).
[9] Zhang Y, Lee W and Huang Y. Intrusion detection techniques for Mobile Wireless Networks, Wireless Networks Journal, Vol. 9,No. 5,2003,pp 1-16.
[10] Intrusion detection Systems, from Wikipedia, the free encyclopaedia, http://en.wikipedia.org/wiki/Intrusion-detection_system.
[11] 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.
[12] M.G Zapata, "Secure Adhoc On-Demand Distance Vector(SAODV) Routing," ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp.106-107, July 2002.
[13] Y.Hu, D.B Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp.3-13, June 2002.
[14] Y. Hu, A.Perrig, and D.B Johnson, "Ariadne: A secure On-Demand Routing Protocol for Adhoc Netwroks," Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002.
[15] A.Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5 (Summer), 2002.
[16] S.Madhavi and Tai Hoon Kim, "An Intrusion Detection System in Mobile Adhoc Networks", International Journal of Security and Its Applications Vol. 2, No. 3, July, 2008.
[17] Tseng C.H, Wang S.H, Ko C, Levitt K, "DEMEM: Distributed Evidence Driven Message Exchange Intrusion Detection Model for MANET", RAID 2006, LNCS 4219, Springer, pp 249-271, 2006.
[18] Huang Y, Lee W, "Attack Analysis and Detection for Adhoc Routing Protocols", RAID 2004, LNC 3224,pp 125-145 Springer, 2004.
[19] Martuza Ahmed, Rima Pal A.NIDS: A network based approach to intrusion detection and prevention A.IEEE 2009.

