ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)
Volume 2, Issue 9, September 2013

INTRUSION DETECTION AND RESPONSE IN MANET ROUTING ATTACKS

M.MANJULA[1] , K. RAVIKUMAR[2]

1 RESEARCH SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE,
TAMIL UNIVERSITY, THANJAVUR.

2 ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE,
TAMIL UNIVERSITY, THANJAVUR.

Abstract __ Mobile Ad Hoc Networks (MANET) is varied from other networks mainly by its self-configuring and self-optimizing nature. Being the flexible network, MANET is exposed to various types of attacks mainly the routing attacks is currently in the networking system. To reduce certain attack possibilities, prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defense . An Intrusion detection system observes and evaluates the activities of the nodes and determines the performance with the security rules. An Intrusion Detection System will alert the neighbor nodes if any problem arises in the performance of a node. An intrusion Response System will take further actions on recovering the affected services and reconfigure the system. Due to the continuous change in topology and an open vulnerable media network, achieving security in ad hoc networks is very difficult.

Keywords −Mobile ad hoc networks, intrusion response mechanisms, intrusion detection systems.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) that is scattered and the self-configuring wireless network. MANET does not have a predefined network infrastructure. Application of MANET is benefited in areas such as military services, disaster relief and mine site operations. Each node communicates with the other acting as routers. The co-operation between the nodes are depending for the proper functioning of this network. Since the network topology in MANET changes unpredictably and rapidly it is highly vulnerable to various kinds of attacks. Attack prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defense for reducing certain attack possibilities. MANET is considered as one of the most promising fields in research and development of wireless networks. The existing techniques usually attempt to isolate the malicious nodes from the topology there by causing the partition of network topology.

Methods such as binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET.

Several intrusion detection techniques have been introduced for detecting the malicious nodes and preventing the neighbor nodes compromised by the malicious nodes. Even though many mechanisms and routing protocols are introduced each of them has one or more vulnerabilities. When a malicious node is being identified the node has to be repaired or any other route has to be established. In most of the existing techniques the nodes when found slightly malicious is completely isolated from the network which will make splitting of the network and thereby causing communication problems between the nodes.

II. INTRUSION RESPONSE MECHANISM

Several techniques have been put provided for better performance of MANET. The methods include detection, prevention and evaluation of various kinds of attacks and malicious nodes in the network. The main goal of an Intrusion Response System is to recover the affected nodes and reconfigure that nodes.

The risk aware response mechanism is divided into the following four steps:

2.1 Evidence collection:

Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table

Change Detector (RTCD) runs to detect the number of changes on the routing table that is caused by the attack. This identifies as well as evaluates the problem which is caused by the intruders. 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. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and determining intruders from violating security policies.

2.2 *Risk assessment*:

The aware confidence for assessing the risk from IDS and the routing table that changes the data would be more consider as independent evidences for the risk factor computation and united with the extensive D-S model. Risk of countermeasures is calculated during a risk assessment phase. Depending on the risk factors of routing attacks and the countermeasures, the whole risk of an attack could be figured out for making changes.

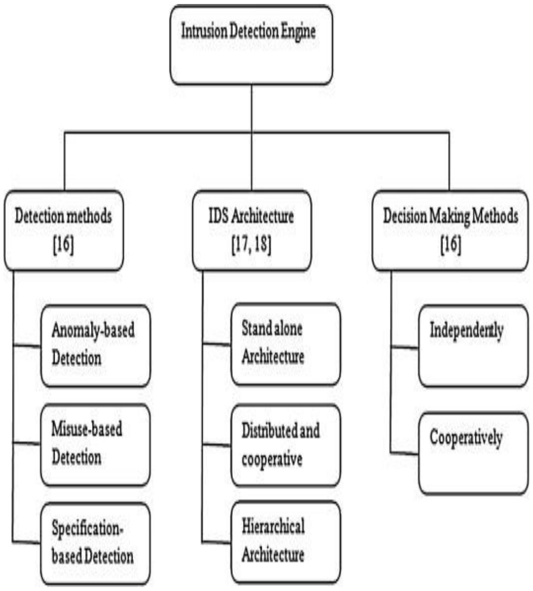
2.3 *Decision making*:

The adaptive decision making module provides a flexible response decision - making mechanism, that takes some risk evaluation and risk tolerance into the account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

2.4. Intrusion Response:

With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner routing attacks.

To overcome those attacks ADRS and pathrater techniques have been introduced in the following sections. To enhance the MANET performance, these methods are provided to monitor and rectify the attacks caused when transferring Packets over network.


Intrusion Detection Engine
Detection methods [16]
IDS Architecture [17, 18]
Decision Making Methods [16]
Anomaly-based Detection
Misuse-based Detection
Specification-based Detection
Stand alone Architecture
Distributed and cooperative
Hierarchical Architecture
Independently
Cooperatively

III. ANOMALY DETECTION SYSTEM (ADS)

Anomaly Detection System plays a important role in detecting the anomalous actions of attacks in Mobile Ad hoc Network. The autonomous nodes in MANET work independently and cooperatively with each other. It is distinguished from the other network counterparts on four functional roles: self-configuration, self - healing, self - optimization and self-protection ADRS analyses the MANET anomalies resulted by both intentional and unintentional or accidental attacks such as traffic congestion, signal interference etc. ADRS will monitor the node performance and analyze the behavior of the nodes. Based on the analysis and detection the corresponding responses are made.

Each Anomaly Detector (AD) in an ADRS monitors the behavior and traffic of the neighboring nodes and shares the information between the other AD's. The overhead is negligible due to light weight of AD's. The behavior of the node is determined by the packet forwarding ratio. The major parameter for an ADRS detecting the node behaviour is based on a threshold value which determines the distance between the regularity of monitored events and that of normal profiles. Some other parameters associated with detection and response is also examined for improving the accuracy of the model. ADRS is evaluated by means of detection accuracy and false positive rate, operation cost including both detection cost and cost for response is one another important factor, is always ignored. However, in fact, this metric is extremely important in MANET in that its network node usually have scarce resource, an ADRS consuming non-negligible overhead would be undesirable. More seriously, as each network node is autonomous, it may refuse to run an ADRS sensor if the overhead impedes its normal operations. Henceforth, from a systematic viewpoint, it is a significant issue to explore the tradeoff between detection performance and operational cost (and other metrics) of an ADRS, so that the best detection performance can be achieved with the minimum operational cost. no other central authority involved. implies the following facts:

Each AD monitors local traffic and the behavior of its neighbors, and it shares and exchanges the information with other Ads for correlating events and coordinating responses against an observed anomaly. Impacted by both detection algorithms and observations, AD varies in detection coverage and blind spot.AD is light-weight, consuming negligible overhead. Each AD is expected to capture the drifts of a node’s normal profile, enabling ADRS to adapt to the dynamic network environment. ADRS is expected to be operating in secure and dependable manners, avoiding the introduction of new vulnerabilities which may allow sophisticated attackers to compromise ADRS. Also, the failure of AD should not result in performance deterioration of the whole ADRS.

IV. WATCHDOG AND PATHRATER

Throughput is an important factor in ad hoc networks; increase in throughput is an increase in quality of communication. Two techniques, watchdog and pathrater is being used here. Watchdog is a technique that identifies the malicious or misbehaving nodes in a network topology, where as the pathrater will guide the routing protocols to avoid these detected affecting nodes and provides another path. When these techniques are used together in a network this will increase the throughput by 17% in a network with 40% malicious nodes. Wireless communication has a tremendous growth over wired due to its mobility and less expense of hardware and wires. The two techniques are extended to the Dynamic Source Routing (DSR) algorithm to reduce the misbehaving nodes in a network. Watchdog can detect the neighboring node behavior by listening the attack, if every node doesn’t forwarding the packet this will be considered as the misbehaving node.

When node A wants to wants to send packet to S it has to pass through the intermediate nodes B and C. Node A cannot transmit all the way to Node S. The packet is transmitted to Node B and then to Node C. Node B can listen to Node C whether it transmits the packet to Node S.A buffer is maintained, where the recently sent packet is stored and compares each packet overhead with the packet in the buffer to see if there is a match. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node .Pathrater uses the information from the watchdog to check the misbehaving nodes. It picks the most reliable path for the nodes To communicate. It contains a node rating based on which the path consistency mechanism is calculated. Without an active watchdog the pathrater cannot detect misbehaving nodes. Pathrater assigns ratings to nodes according to the following algorithm. When a node behaviours in the network is known to the path rater . This work encompasses the existing technique of MANET using the combination algorithm. The new technique of pathrater determines the attacked nodes and checking for rectifying the nodes.

V. MONITOR ANALYSIS DETECTION RESPONSE

The pathrater increments the ratings of nodes on all actively used paths by 0.01 at regular intervals of 200 ms. An actively recycled path is the one on which node has seen a packet within the previous rate increment interval. The maximum value that a neutral node will achieve is 0.8. The decrement of a node's rating by 0.05 when it detect a link break when the packet is forwarding and the node will be unreachable. The minimum bound ranking of a "neutral" node is 0.0. The pathrater does not modify the ratings of nodes that are not currently in active use. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the percentage of overhead transmission from 12% to 24%.

VI. CONCLUSION

MANET is distinguished from other networks mainly by its self -configuring and optimizing nature. The flexible network that contains and describes MANET is exposed to various types of attacks mainly the routing attacks. MANET contains many different methods that is introduced to mitigating such critical attacks such as intrusion detection techniques. Some response systems or mechanisms evaluates and analyses the activities of the nodes and determines the performance with the security rules. Once an IDS finds any irregularities in the performance of a malicious node, it automatically generates an alarm alert to the system administrator for the further actions. By the repeated changes in the topology and an open susceptible network, achieve security in ad hoc networks is very complicated. Several techniques have been put forward for better performance of MANET. In MANET situation, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address these critical issues, more flexible and adaptive response should be investigated. At present, the focus of MANET is towards mesh networking and large scale networks. Improvement in various areas such as security and bandwidth is required. The further analysis for improving MANET performance and to avoid node reputation in this decision model.

VII. REFERENCES

[1] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, page 86, 2007

[2] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidence driven message exchange intrusion detection model for manet. In Recent Advances in Intrusion Detection, pages 249–271. Springer, 2006.

[3] M. Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion detection approach for OLSR MANET protocol. In Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on, pages 55–60, 2005.

[4] S. Wang, C. Tseng, K. Levitt, and M. Bishop. Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks. LECTURE NOTES IN COMPUTER SCIENCE, 4637:127, 2007.

[5] T Ylonen, C Lonvick, The secure shell (ssh) authentication protocol (Request for Comments 4252, MANET Working Group, http://www), . ietf.org/rfc/rfc4252.txt webcite, January 2006

[6] C. Mu, X. Li, H. Huang, and S. Tian.Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, page 48. Springer, 2008.