An Overview on Intrusion Detection in Manet

Rajesh D. Wagh
Computer Sci. and Engineering
SYCET
Aurangabad (MH), India
rajesh.wagh11@gmail.com

Swapnil D. Kurhe
Computer Sci. and Engineering
SYCET
Aurangabad (MH), India
swapnil.kurhe@gmail.com

Saurabh R. Dahake
Computer Sci. and Engineering
SYCET
Aurangabad (MH), India
saurabhdahake25@gmail.com

Abstract

A mobile ad hoc network (MANET) is a self-configuring of mobile devices network connected without wires and hence MANET has become a very popular technology now days. A MANETS are the networks that are building, when some mobile nodes come in the mobility range of each other for data transfer and communication. In MANET, nodes are not stable hence the communication topology is not stable due to this vulnerable for attacks. MANET devices are connected via wireless links without using an existing network infrastructure or centralized administration due to which MANETs are not able to diverse types of attacks and intrusions. Hence intrusion detection has attracted many researchers. This paper gives an overview and different methods to detect intrusion in MANET.

Keywords-MANET, self-configuring, intrusion, network**.**

I. INTRODUCTION

MANETS is a network consisting of mobile nodes such as Laptop, PDAs and wireless phones with the characteristics of self-organization and self-configuration [6]. Mobile ad hoc networks (MANET) are also known as spontaneous networks. MANETS are collection of dynamic cooperating peers and which consist one of the most promising wireless technologies. In MANETS, the mobile devices create a wireless communication channel. The mobile devices contribute in the routing decisions of the network since there are no central stations. Mobile nodes communicate directly with nodes in their vicinity and they relay messages on behalf of others to enable communication with devices not in direct radio-range of each other [2].

Ad hoc networks suffer from a great weakness: due to their characteristics, they are much more vulnerable than wired networks, because of an open medium and have a very dynamically changing topology. MANETs are vulnerable to many kinds of attacks such as passive eavesdropping, DoS, and usurpation. Recently, many schemes have been proposed to prevent different attacks like; cryptographic mechanisms to authenticate participants within the network. Cryptographic mechanisms may help to identify the originators of an attack but we not only needs to prevent attacks but also to detect the incorrect behaviors in real time. This is done by using IDS [7]. Intrusion detection is nothing but a process of monitoring activities in a system. The mechanism by which this is achieved is called an intrusion detection system (IDS) which collects activity information and then analyzes it to determine whether there are any activities that violate the security rules and also IDS can also initiate a proper response to the malicious activity. If any activity is found, an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. These systems alert the network that an intrusion may take place and then take direct reactive and preventive measures to protect the network from different intrusion and it is useful to improve the security policies used to detect the possible threats and points of failure in the network. The main challenge is to construct intrusion detection and response solutions while preserving the desired network performance [8].

II. TYPES OF ATTACKS IN MANETS

There are different attacks in MANETS that target some particular routing protocols and these attacks are classified according to network protocol stacks. Table 1 show an example of a classification of security attacks based on protocol stack and some attacks could be launched at multiple layers [9].

TABLE I. CLASSIFICATION OF SECURITY ATTACKS [9]

Sr. No.	Layers	Attacks
01	Application layer	Repudiation, data corruption
02	Transport layer	Session hijacking, SYN flooding
03	Network layer	Wormhole, Black hole, Byzantine, flooding, location disclosure attacks
05	Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
06	Physical layer	Jamming, interceptions, eavesdropping
07	Multi-layer attacks	DOS, impersonation, replay, man-in-the-middle

III. RELATED WORK

Nisha Dang and Pooja Mittal [1] proposed a Cluster based intrusion detection system. This system is designed to restrict the intruder's activities in clusters of mobile nodes. In this system each clusters each node run some detection code to detect local as well as global intrusion. In this paper, system has taken insight of intrusion detection systems and different attacks on MANET security. System proposed a generalized clustering algorithm that can run on top of any routing protocol and can monitor the intrusions constantly irrespective of the routes. Clustering scheme has been used to detect intrusions in the MANETS, resulting in high detection rates and low processing. Proposed system also detects memory overhead irrespective of the routes, connections, traffic types and mobility of nodes in the network.

Marjan Kuchaki Rafsanjani el at [2] proposed an hybrid system that is it not only prevention internal intruder but also detect external intruder by using game theory in mobile ad hoc network (MANET). Cluster head for each cluster is elected by one optimal solution for reducing the resource consumption of detection external intruder, which provide intrusion service to other nodes in its cluster. These nodes are called normal nodes. Proposed hybrid system has three phases. In the first phase building trust relationship between nodes and estimation trust value for each node to prevent internal intrusion. To prevent internal intrusion neighbouring nodes participate in the game and each node observes treat neighbours then estimates a trust value for them. If the estimated trust value of a node be less than a threshold, then it is detected as a misbehaving node. In the second phase an optimal method for cluster head election by using trust value and in the third phase system finds the threshold value for notifying the victim node to launch its IDS once the probability of attack exceeds that value. In the third phase for detecting external intrusion with minimum cost proposed system introduced a game between cluster head and external intruder based In first and third phase we apply Bayesian game due to using game theory, trust value and honest cluster head election algorithm can effectively improve the network security, performance and reduce resource consumption.

Debdutta Barman Roy, Rituparna Chaki, and Nabendu Chaki [3] proposed cluster-based wormhole intrusion detection algorithm for MANET that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack In MANET there are different types of attacks but particularly devastating attack is the wormhole attack. In this attack a malicious node records control traffic at one location and tunnels it to another compromised node which replays it locally. In ad hoc networks routing security is often equated with strong and feasible node authentication and lightweight cryptography and the wormhole attack can hardly be defeated by crypto graphical measures because wormhole attackers do not create separate packets, they simply replay packets already existing on the network, which pass the cryptographic checks. This paper present a cluster based counter-measure for the wormhole attack.

R.Nallusamy, K.Jayarajan, and Dr.K.Duraiswamy [4] proposed GA Based Feature Selection method for intrusion Detection in Mobile Ad Hoc Networks. Intrusion detection system (IDS) tools are suitable for identifying different attacks in MANET. There are two methods to analyze: misuse detection, is not effective against unknown attacks and anomaly detection. Anomaly detection is more effective against the unknown attacks and therefore this method is mostly used. In this method, the audit data is collected from each mobile node after simulating the attack and compared with the normal behaviour of the system. Audit data is collected from the nodes and if there is any deviation found from normal behaviour then the event is considered as an attack. Proposed system is implemented on two feature selection methods namely, Markov blanket discovery and genetic algorithm. In genetic algorithm, Bayesian network is constructed over the collected features and fitness function is calculated and in the Markov blanket discovery also uses Bayesian network and the features are selected depending on the minimum description length. During the evaluation phase, based on the fitness value the features are selected, the performances of both approaches are compared based on detection rate and false alarm rate.

Nitiket N Mhala and N K Choudhari [5] present an approach for determining conditions under which critical nodes should be monitored. System is focus on the trigger mechanism for the invocation of critical node test for

MANET Intrusion Detection system (IDS). IDS focus on critical node and detection of critical link by using basic routing utilities. In the proposed system whenever a critical link is detected, the host node may choose expend additional resources such as traffic monitoring watchdog module or collaborative IDS to initiate an IDS module that is more resource intensive. This system provides the approach for detecting critical links and which may be used to provide guidance for how the location of nodes in an ad-hoc network might be better physically arranged in order to provide more fault tolerance and better Quality of service.

Farzaneh Pakzad and Marjan Kuchaki [6] classify the techniques for intrusion detection systems (IDS) that have been introduced for MANETs, and compare some important aspects such as performance and overhead in these techniques. This paper provides comparison of different Intrusion Detection Techniques in Mobile Ad hoc Networks such that Watchdog (identifies misbehaving node by eavesdropping on the transmission of the next hop), Pathrater (technique calculates "path metric" for every path), Route guard (employs a smart and smooth architecture in order to effectively discover malicious nodes and then proceeds to protect the network), Hop-by-hop signing (This system proposed a secure routing system which would allow intrusion detection), Patwardhan secure routing and intrusion detection system (This technique presents a proof of concept where a secure routing protocol is implemented by using public key encryption, intrusion detection, and a reaction system), Ex Watchdog (proposed techniques to identify IDS and which is actually an extension of Watchdog), ONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad hoc Networks, which is in fact an expansion of DSR protocol. This technique is similar to Watchdog and Pathrater), CORE (A technique which is proposed to detects selfish nodes and forces them to cooperate as well and Similar to CONFIDENT), OCEAN (Observation-based Cooperation Enforcement in Adhoc Networks, which is an extension of the DSR protocol).

Jean-Marie Orset et al. [7] propose an intrusion detection scheme based on extended finite state machines (EFSM). Proposed system provides a formal specification of the correct behaviour of the routing protocol and by the means of a backward checking algorithm detects run-time violations of the implementation and choose the standard proactive routing protocol OLSR as a case study and show that our approach allows detecting several kinds of attacks as well as conformance anomalies. System proposed a specification based approach that relies on the use of extended finite state machines to detect attacks on the OLSR protocol. Extended finite state machines makes possible to analyze in depth, the messages exchanged between nodes and also applied a backward checking algorithm to detect violations on the specification. This approach provides a significant benefit on the quickness of the verification process, what is crucial in the context of run-time verification. Lastly applied an algorithm to detect flaws on the OLSR protocol and showed that it makes it possible to detect several kinds of anomalies.

Charlie Obimbo and Liliana Maria Arboleda-Cobo [8] paper discusses an enhancement of the Watchdog / Pathrater form of Intrusion Detection in Mobile wireless Adhoc networks (MANET). To detect and avoid malicious nodes in MANET, system implement a schema similar to Watchdog and Pathrater on top of DSR. The participating nodes are allowed to listen to the nodes they have conveyed messages to, in promiscuous mode, if within a certain timeframe the message is not relayed, then the node is suggested to be tagged as a misbehaving node. Depending on the Trustworthiness of the node's sending the tag information, and information already relayed by other nodes, the tagged node may then dropped from routing paths by the Pathrater, and new routes formulated. A simple simulation is done to illustrate the modality of these new IDS for MANET.

Noman Mohammed, [10] this paper presents a secure leader election method for intrusion detection in mobile ad hoc networks (MANETs). To find out the intrusion detection in MANETs there are two problems such as a node might behave selfishly by lying about its remaining resources and avoiding being elected and electing an optimal collection of leaders to minimize the overall resource consumption may incur a prohibitive performance overhead. For the optimal election and selfish node issues system uses two possible application settings that is Cluster Dependent Leader Election (CDLE) and Cluster Independent Leader Election (CILE). For finding selfish nodes, provide a new solution which is based on mechanism design theory i.e. it is based on the Vickrey, Clarke, and Groves (VCG) model to ensure truth-telling to be the dominant strategy for any node. Paper presents a series of local election algorithms that can lead to globally optimal election results for addressing the optimal election issue. For these issues there are two kinds of settings, first one is Cluster Dependent Leader Election (CDLE) and second one is Cluster Independent Leader Election (CILE) and finally results showed that our model is able to prolong balance the overall resource consumptions among all the nodes in the MANETS. Methods are able to decrease the percentage of leaders, single node clusters, and maximum cluster size and increase average cluster size which is useful to improve the detection service through distributing the sampling budget over less number of nodes and reduce single nodes to launch their IDS.

IV. CONCLUSION

This paper focused on Intrusion detection in MANETs and related work provides an overview about the various existing methods for the intrusion detection.

REFERENCES

[1] Nisha Dang and Pooja Mittal, "Cluster Based Intrusion Detection System for MANETS", IJCAIT, Vol. 1, No.1, July 2012, pp.16-18.

[2] Marjan Kuchaki Rafsanjani, laya Aliahmadipour and Mohammad Masoud Javidi, "A hybrid intrusion detection by game theory approaches in MANET", Indian Journal of Science and Technology, Vol. 5 No. 2, Feb 2012, pp.2123-2131.

[3] Debdutta Barman Roy, Rituparna Chaki, and Nabendu Chaki, " A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.pp.44-52.

[4] R.Nallusamy, K.Jayarajan, and Dr.K.Duraiswamy, "Intrusion Detection in Mobile Ad Hoc Networks Using GA Based Feature Selection", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 2009, pp.28-35.

[5] Nitiket N Mhala and N K Choudhari, "An Approach for Determining Conditions for Monitoring of Critical Nodes for MANET Intrusion Detection System", International Journal of Future Generation Communication and Networking Vol. 4, No. 1, March 2011,pp. 55-59.

[6] Farzaneh Pakzad and Marjan Kuchaki Rafsanjani, "Intrusion Detection Techniques for Detecting Misbehaving Nodes", CCSENET, Vol. 4, No. 1, January 2011, pp. 151-157.

[7] Jean-Marie Orset, Baptiste Alcalde, and Ana Cavalli, "An EFSM-based intrusion detection system for ad hoc networks", ATVA, 2005, pp.400-413.

[8] Charlie Obimbo and Liliana Maria Arboleda-Cobo, " An Intrusion Detection System for MANET", CISME Vol.2 No.3 2012 PP.1-5.

[9] Vinay P.Virada, "Intrusion Detection System (IDS) for Secure MANETs: A Study",IJCER, Vol. 2 Issue. 6, 2012, pp. 75-79.

[10] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya, " Mechanism Design-Based Secure Leader ElectionModel for Intrusion Detection in MANET", IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, 2009, pp. 1-15.