Intrusion Detection Techniques in Mobile Adhoc Networks: A Review

Salman Naseer
University of the Punjab, Gujranwala Campus, Pakistan
Email: salman@pugc.edu.pk

Rashid Mahmood
University of Gujrat, Pakistan
Email: rashidbaryar@gmail.com

***Abstract*—Mobile ad hoc networks (MANETs) use has been well-known from the last few years in the many applications, like mission critical applications. In the (MANETS) prevention method is not adequate as the security concerned, so the detection method should be added to the security issues in (MANETs). The authentication and encryption is considered the first solution of the MANETs problem where as now these are not sufficient as MANET use is increasing. In this paper we are going to present the concept of intrusion detection and then survey some of major intrusion detection techniques in MANET and aim to comparing in some important fields.**

***Index Terms*—MANET, IDS, intrusions, signature, detection, prevention**

I. Introduction

A mobile ad hoc network (MANETs) is that type of network which is self configure and does not have a fixed infrastructure or cartelized management. Every device or equipment is connected with other devices through the wireless link. And every device has node a move onward a packet to node which is out of radio range the cooperation of the other nodes which is called as multi hop communication. Due to that every node is act like as a host node and also router [1], [2].

The characteristic of the MANETs was developed for military point of views [3]. One node is scattered in the battle field where there is no infrastructure are there which is form a network. This network developed without any infrastructure but on other hand ranging from military to civilians and also commercial aspect. Due to wide use of the MANETs there is security is primary objective. In the most MANETs routing protocol presume that every node is cooperative in the network and not malicious [4].

Intrusion Detection models were established in 1987 [5]. The intrusion detection models have two type: Signature based intrusion detection and anomaly based intrusion detection. In the *signature based intrusion detection* the intrusion uses the signature of attacks. In the *anomaly based intrusion detection* monitor the whole network and also compare the network traffic and attack pattern [6]. It also produce profile based of network whose shows the normal behaviors. Advantage of this type detection it is detects new attack with any earlier knowledge [7].

In MANETs both of attacks approaches are exist one is passive and other is active. In passive approach the attacks packets violate the privacy of data. On other hand the active approach attacks packets disturb or change the location in network, deleting packets and modify packets data. The cryptography and authentication [8], [9] are used in pro active approach were produced from assumption and also proposed many techniques. If we have capacity to prior detect the attack into the network then we are in position to stop and it from any loss of data and as well as system. In intrusion detection system monitors the whole network and also individual system. The IDS find the any uncertain activity that is the cause of any attack occurs the system will generate the call to the security administrator [10], [11].

In the very early stages the system are not more complex and there are only use the prevention techniques [12] such as encryption and authentication which are not sufficient on defense purpose. When the system is become more complex the intrusion became the major issue [13], so the detection of the intrusion is the second wall of the defense which protects the network. There is much assumption prepared about the intrusion detection system [1] such as observable, intrusion activities are distinct behavior.

The IDS based on detection techniques are have three forms which are given below [2]:

A. Anomaly Detection System

This type of intrusion is working on the normal behavior and system compare with captured data with normal behavior and treats with any activity response by the baseline and also informs the system administrator.

B. Misuse Detection System

In this type the system will remain the signature of the attacks node and compare with the captured data, if it is match then system treats as the intrusion.

Manuscript received June 9, 2014; revised July 11, 2015.

doi: 10.18178/lnit.3.1.52-55

C. *Specification Based Detection*

In this type the system set some parameter about the intrusion and stores it after the compare of data if it is match then system take action according to the set of constraints. The classification of intrusion detection system is based on the network and also on host. A critical analysis is given below Fig. 1.

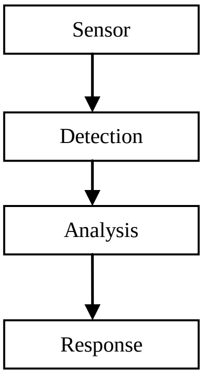

Figure 1. Intrusion detection system

The host based IDS take portrait of whole system and associate with old one due to that its overburdened, not see packet headers but detect attacks before knock of network. Other hand network based NIDS works on subnet base if detect someone compare with subnet's attacks library so that its host independent, observe packets but detect attacks load analyzed network see the Table I.

TABLE I. COMPARISON OF HOST AND NETWORK BASED IDS

Host based IDS	**Network Based IDS**
Over burdened	Never Over burdened
Host depended	Host Independent
Not see packet headers	observe the packets
Low false + rate	High false + rate
Detect attacks before knock of network	Detect attacks load is analyzed the network

II. RESEARCH METHODOLOGY

In this review paper we describe here different architectures of Intrusion Detection System Architectures form history and literature and different techniques implementing these architectures. At the end we compare these techniques.

A. *Architecture of IDS*

The architecture of the IDS is depending on the nature and the type o f the network. If the network is wired the architecture of IDS in that scenario is control the devices. The architecture of IDS in wired network is based on devices and these devices are the major part of the network. On the other hand in MANETs the infrastructure is totally changed. The network infrastructure of MANETs divided in to two categories one is flat and second is multi relay. In the first part which is flat infrastructure all the nodes are treat as same on the other hand nodes may have divide in different cluster [14]. Here are some architecture for IDS in MANETs given below.

1) *Stand alone IDS*

In this type of the architecture for IDS is based on the every node because every node has IDS to detect intrusion. No node knows the actual status of the other node which is part of the network infrastructure. So due to this thing that techniques is not reliable in multi rely and used in flat techniques.

2) *Distributed and cooperative IDS*

The distributed and cooperative IDS technique is much better than stand alone because in this every node which is the part of network is cooperate with other nodes. Every node participates to find the intrusion in the network. This work is done by the help of the agent IDS which is running on the every node Like the proposed model [15].

3) *Mobile agent for IDS*

The MAs are used in several techniques for intrusion detection system in MANETs. Every MA assigns a work and many MAs working in the network. There are many advantages of mobile agent [6]. Some node is not having MA because such these type of resolve problem itself. Architecture of Mobile agent is shown in Fig. 2.

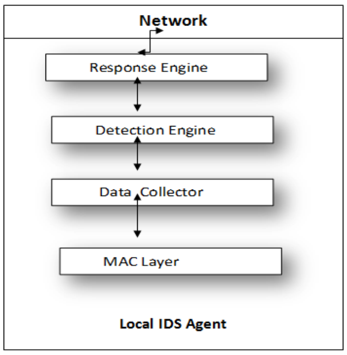

Figure 2. Mobile agent for IDS

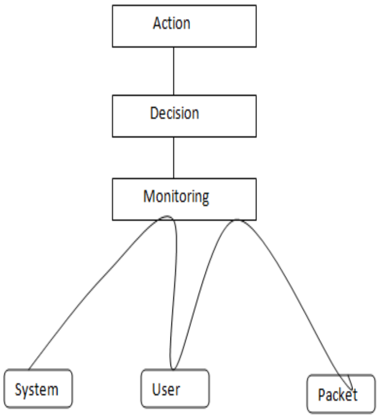

Figure 3. Hierarchical IDS

4) *Hierarchical IDS*

The hierarchical IDS [16] are more reliable form of the distributed or cooperative IDS, because this type is used for the multi layered purpose. Where the multi layer is divided in to clusters and head clusters. The cluster head is responsible to monitor the cluster and the cluster is responsible to convey the information about the intrusion in the network, see the Fig. 3.

5) Zone based IDS (ZBIDS)

The Zone Based intrusion Detection System proposed by Steren *et al* [17]. In this technique the network is divided into the zone and all other activity are perform in the related zone. Nodes are categories in to two types one is interzone node and second is intrazone nodes.

B. Intrusion Detection Techniques in MANETs

In The MANETs no infrastructure has exists due to that reason each node is cooperate with other node for forwarding of the packet which is received. But on other hand some nodes are changed or damaged the packet due to misbehavior. The simulation is [18] shows that some node are act as like misbehavior node which is degrade the overall performance of the network. There are some techniques are given for IDS in MANETs.

1) Watchdog and pathrater

Watchdog and pathrater are both planned by the Marti and Bakar [16], in the first techniques find the misbehaving node in the network and on other hand the Pathrater find that route where the misbehaving node are not exist. Bothe techniques are used in DSR [19]. In the DSR the information is reach to destination by using intermediate node which kept all the information about the destination and next hope node. On other hand the parthrater is find path metric of each path. The path metric find by the calculated the reliable rating of the node which is calculated by the old experience by the node. Pathrater are chosen the highest path metric node as the result avoid the misbehaving node in the paths.

2) Core

In this type of the IDS technique find the special type of the misbehaving node which is selfish node. Core is also forced that type of the node to cooperate other node. Core is monitoring and a reputational technique which is monitors the network and set the reputational table. This technique is proposed by Molva [20].

3) Ocean

Ocean stand for Observation based Cooperation Enforcement in ad hoc Network, this techniques is introduced by the Bansal and Baker. Ocean is also monitoring and reputational technique. The ocean is believed on its observation to avoid the new misbehaving from second hand reputational exchange. Due that this technique has standalone architecture. Ocean has two types one is misleading and second is selfish [21].

- Misleading ocean

In this type of ocean the node find only route discovery but no forward a packet this is known as misleading.

- Selfish ocean

If the node does not participate in the route discovery this is known as selfish ocean.

1) Confidant

CONFIDANT stands for Cooperation of Nodes, Fairness In Dynamic Ad hoc network. This technique is projected by the Buchegger and Leboudec in extension to the DSR. This technique is also like the Watchdog and Patrather working with the help of the behavior of neighbor node. But on other hand it is punished to the misbehave node. This technique is working as two terms one is observation and second in trusted [22].

- Observation

In this type find the hateful behavior node within the radio range. If rating rate of that node is unacceptable the system ALRAMS the message to trust manager.

- Trusted

When monitor receives ALARMS form its friend first its check the level of the trustworthiness. If the message is trustworthy then send it to the ALARM table and if it is not then maintain its reputational table.

C. Comparison of Intrusion Detection Techniques in MANETs

In this Table II we compare different techniques of IDS Watchdog/Pathrater, Cooperative, Ocean, Core and Confidant from the literature. On the basis of different parameters Architecture of techniques, Data distribution, Type of data, Network Throughput, Avoid misbehave node, Observation, Punishment, Second chance of Mechanism and False Accusation

TABLE II. COMPARISON OF INTRUSION DETECTION TECHNIQUES IN MANET

Name Of Techniques		**Watchdog/ Path rater**	**Cooperative**	**Ocean**	**Core**	**Confidant**
Architecture Of Techniques		Distributed & Cooperative	Hierarchical	Stand alone	Distributed & Cooperative	Distributed & Cooperative
Data distribution		Negative to source	Cluster head	NO	Positive (Rrep.)	Negative to friend
Type Of Data		Reputation	Statistics	Reputation		
Network Through put		NIL	NIL	Higher in defenseless reputation	Higher in DSR	Higher in DSR
Avoid misbehave node		No	NIL	Yes	No	No
Observation	**Individual To Neighbor**	YES	YES	YES	YES	YES
	Neighbor To Neighbor	NO	NO	YES	NO	NO
Punishment		Nil		YES		
Second Chance of Mechanism		NO	NO	NO	YES	YES
False Accusation		Restricted	Restricted	Restricted	Restricted	Can not Restricted

In the above IDS techniques the watchdog technique is most frequently used in all of them but on other hand the watchdog technique is also cannot work properly in the occurrence of crash. Watchdog also cannot determine accurately when the transmission rang is different. All the IDS techniques shows a common role on detecting the selfish nodes, where as OCEAN cannot find the misbehavior node.

III. Conclusion

As we discussed before, MANETs is a set of nodes that they are at random located in operational location without any infrastructure. Nodes hadn't any information about surroundings, then each node is active, they try to recognize other neighboring nodes in location and join the MANET in the cluster. By concentration to this said notice, MANETs are susceptible to a variety of attacks. In this review describes the IDS techniques which are working to find the misbehavior nodes and also selfish nodes, which is totally depending on the MANETs approaches. A great comparison are should take place in this paper which is more beneficial for monitoring, detecting and also solving the much more security issues of MANETs. The main aim of the IDS is to detect the attack on mobile node and also safe from the intrusion to the network.

References

[1] R. Chandra, L. Qiu, K. Jain, and M. Mahdian, "On the placement of internet taps in wireless neighborhoowed networks," in *Proc. ICNP*, 2004.

[2] J. Boyer, D. D. Falconer, and H. Yanikomeroglu, "Multihop diversity in wireless relaying channels," *IEEE Transactions on Communications*, vol. 52, no. 10, pp. 1820-1830, October 2004.

[3] D. S. Alberts and R. E. Hayes, *Washington DC: Command and Control Research Program*, 2004, pp. 125.

[4] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," *Journal of Wireless Networks*, vol. 9, no. 5, pp. 545–556, 2003.

[5] D. E. Denning, "An intrusion detection model," *IEEE Transactions in Software Engineering*, vol. 13, no. 2, pp. 222-232, 1987.

[6] F. Anjum, D. Subhadrabandhu, and S. Sarkar, "Signature-based intrusion detection for wireless ad-hoc networks," in *Proc. Vehicular Technology Conference*, USA, Oct. 2003, vol. 3, pp. 2152-2156.

[7] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Ti-wary, H. Yang, and S. Zhou, "Specification-based anomaly detection: A new approach for detecting network Intrusions," in *Proc. 9th ACM Conference on Computer and Communication Security*, USA, 2002, pp. 265-274.

[8] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) routing," *ACM Mobile Computing and Communication Review*, vol. 6, no. 3, pp. 106-107, July 2002.

[9] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEE Workshop on Mobile Computing Systems and Applica-tions*, June 2002, pp. 3-13.

[10] S. Marti, *et al*., "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MOBICOM*, 2000.

[11] H. Deng, W. Li, and D. P. Agrawal, "Routing security wireless ad hoc networks," *IEEE Communications Magazine*, vol. 2, no. 1, 2002.

[12] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Information Management & Computer Security Journal*, 2010.

[13] H. Debar, M. Dacier, A. Wespi, and S. Lampart, "A workbench for intrusion detection systems," *IBM Zurich Research Laboratory*, Ruschlikon, Switzerland, March 1998.

[14] S. Sahu and K. Shandilya, "A comprehensive survey on intrusion detection in MANET," *International Journal of Information Technology and Knowledge Management*, vol. 2, no. 2, pp. 305-310, 2010.

[15] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," *ACM/Kluwer Wireless Networks Journal*, vol. 9, no. 5, September 2003.

[16] B. Pahlevanzadeh and A. Samsudin, "Distributed hierarchical IDS for MANET over AODV+," in *Proc. IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, Penang, Malaysia, 14-17 May 2007.

[17] X. Wang, T. L. Lin, and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, USA, 2005

[18] D. E. Denning, "An intrusion detection model," *IEEE Transactions in Software Engineering*, vol. 13, no. 2, pp. 222-232, 1987.

[19] D. B. Johnson and D. A. Maltz, "The dynamic source routing protocol for mobile ad hoc networks (internet-draft)," *Mobile Ad-Hoc Network (MANET) Working Group*, October 1999.

[20] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. Com-munication and Multimedia Security Conference*, September 2002.

[21] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc. Seventh Int'l Workshop Security Protocols*, 1999.

[22] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol (cooperation o nodes - Fairness in dynamic ad-hoc networks)," in *Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, June 2002, pp. 226-336.

Mr. Salman Naseer completed his M.Sc. Computer Science from Punjab University College of Information Technology, University of the Punjab Lahore Pakistan in 2004. He is currently pursuing MS leading to PhD in Computer Science (Specialization in Computer Networks) from Lahore Leads University, Pakistan. He is working as a Lecturer in the Department of Information Technology, University of the Punjab, Gujranwala Campus. Currently he is doing research in the field of Vehicular Adhoc Networks regarding issues in MAC layer and routing protocols in VANETs.

Mr. Rashid Mahmood has completed his M.Sc. in Information Technology from University of the Punjab, Gujranwala Campus, Pakistan. Now he is currently doing MS in Computer Science (Specialization in Computer Networks) from University of the Gujrat Pakistan. Currently he is doing research in the field of Vehicular Adhoc Networks regarding issues in MAC layer and routing protocols in VANETs