ISSN:0975-9646

A Survey on IDS Techniques to Detect Misbehavior Nodes in Mobile Ad-hoc Network

Sarika Patil[1], Deepali Borade[2]

[1]*M.E (Computer Network), Computer Engineering Department, Flora Institute of Technology, Pune, Maharashtra, India*

[2]*Assistant Professor, Computer Engineering Department, Flora Institute of Technology, Pune, Maharashtra, India,borade*

Abstract-MANET is tremendous increasing area now days for researcher in mobile computing and wireless technology. Mobile Ad-hoc Networks (MANETs) is group of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station. Since of MANET challenges, such as mobility and dynamic nature it is not secure network. MANET is more open to different types of attacks and security threats because of its characteristics. Nodes in a Mobile Ad-hoc Network usually help to other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. . Intrusion is set of action that attempts to compromise the integrity, confidentiality, availability of recourses. Therefore, some novel solutions are required to make Mobile Ad-hoc Network secure. Intrusion Prevention is first step to make the system safe from attack by using passwords, authentication, biometric etc. There is need to second technique to detect and take necessary action on different types of attacks known as IDS. In this paper we have described different types of attack, existing IDS systems categorization and survey on intrusion detection systems for node co-operation in MANET.

Index Terms: Attacks, Dynamic Source Routing (DSR), Intrusion Detection System (IDS), Mobile Ad-hoc Network, Security.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a self configuring network created without human intervention by a collection of mobile nodes. Each node is prepared with a wireless transmitter and receiver, and it allows communicating with other nodes in its same radio range. Each node acts as host and a router at the same time in MANET. The characteristics of MANETs are dynamic topology, security, power consumption, etc. Due to the mobility and dynamic nature of MANET, network is not secure. There are two types of attacks in MANETs such as passive and active attacks. In passive attacks, packets including secret information might be overheard something, and it violates confidentiality. In active attacks, containing introducing packets to unacceptable destinations into the network, removing packets, changing the contents of packets, and masquerading as other nodes violate availability, integrity, authentication, and non-repudiation. Intrusion Detection System (IDS) can be defined as the process of monitoring activities in system, which can be a computer or network system. In this, due to the restrictions of most MANET routing protocols, nodes in MANETs suppose that other nodes always assist with each other to transmit data. This supposition disappear the attackers with the opportunities to achieve major force on the network with just one or two compromised nodes. To tackle this problem, IDS should be added to develop the security level of MANETs. Intrusion detection can be used as a second wall of defense to defend the network from such problems. If the intrusion is found, a response can be started to avoid damage to the system.

Hear focus is on on-demand routing protocols for MANETs, in which a node attempts to determine a route to some destination only when it has a packet to send to that destination. On demand routing protocols have been exhibited to achieve better with considerably lower overheads than proactive routing protocols. Dynamic source routing protocol [2] suggests a number of possible advantages over conventional routing protocols such as distance vector in an ad hoc network.

This paper is organized as follows. Section 2 MANET Security issues. Section 3 Security Schemes in MANET Section 4 discuss different types of IDS for Node Co-operation in MANET. Finally Section 5 conclusion.

2. MANET SECURITY ISSUES

Due to dynamic nature of the MANETs, is vulnerable to different types of attacks and security threads. Security criteria in MANETs are Integrity, availability, authentication, non-repudiation. These are define as

(i) Availability: It define the property of the network to continue provide the services and it is not depend on the state of the network. Ex- denial of service attacks.

(ii) Integrity: Integrity define that no modification, no addition, no deletion, no altering is done to the message but if the altering of message done then it is because of malicious or accidental.

(iii) Confidentiality: Confidentiality defines that the any unauthorized person cannot be viewed the message in its original form.

(iv)Authenticity: It helps to the parties prove their identities. This property ensures that the parties are genuine not impersonators.

(v) Non repudiation: This defines that the sender and receiver cannot disavow about sending and receiving the message, means nobody can read the message.

(vi)Authorization: This property assigns or supports to the different access rights to different types of users.

(vii) Anonymity: All the information about the identification of a node or user should be kept private for privacy preservation.

3. SECURITY SCHEMES IN MANET

3.1. Techniques to secure MANETs:

There are two techniques that are the most common approaches today are:

A. Prevention: Prevention mechanisms usually require encryption techniques to provide authentication, integrity, etc. Some proposals use symmetric algorithms, asymmetric algorithms, and one way hashing.

Asymmetric cryptography: SAODV (Secure Ad-hoc On-demand Distance Vector) and ARAN (Authenticated Routing for Ad hoc) are two protocol proposed in this category. SAODV secures the AODV protocol by digitally signing the fields of the routing message, for authentication. ARAN makes use of the cryptographic certificate to offer the routing certificate. Prevention can be done using Symmetric cryptography protocols under this category are SAR (Security Aware Ad-hoc routing) and SRP (Secure Routing Protocol). SAR attempts to use the traditional shared symmetric key encryption, and involves some sort of key distribution system. Prevention using one-way hash chain: SEAD (Secure Efficient Distance Vector Routing) and Ariadne are two protocols that use this mechanism. SEAD implements one way hash chains to protect modification of routing information like sequence number and source route. Ariadne relies on efficient symmetric cryptography.

B. Detection and Reaction: These are solutions that attempt to identify the malicious activities in the network and take actions against such nodes. e.g include Byzantine, Confidant, DSR, CORE, and using watchdog and pathrater Intrusion Detection System.

3.2. Intrusion Detection System

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an Intrusion Detection System (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. These are the different IDS Techniques.

1. **Anomaly detection systems**: The normal profiles of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
2. **Misuse detection systems:** The system keeps patterns of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.
3. **Specification-based detection:** The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

3.3 IDS Architectures

Based on the network infrastructures, the MANET can be configured to either flat or multi-layer. In flat network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. On the contrary, some nodes are considered different in the multi-layered network infrastructure. Nodes may be partitioned into clusters with one cluster head for each cluster. To communicate within the cluster, nodes can communicate directly. However, communication across the clusters must be done through the cluster head. This infrastructure might be well suited for military applications. There are four main architectures [1] on the network as follows:

1. **Stand-alone architecture:** IDS runs on each node to determine intrusions independently. There is no cooperation and no data exchanged among the IDS on the network. This architecture is also more suitable for flat network infrastructure.
2. **Distributed and collaborative architecture:** Has a rule that every node in the MANET must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.
3. **Hierarchical architecture:** This is an extended version of the distributed and collaborative IDS architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks.
4. **Mobile agents:** have been deployed in many techniques for IDSs in MANETs. Due to its ability of moving in network, each mobile agent is considered for performing just one special task and then one or more mobile agents are distributed amongst network nodes.

3.5 Attacks in MANET

In MANET there are passive and active attacks. The Passive attacks consist eavesdropping of packets and the active attacks consist of actions performed such as replication, modification and deletion of exchanged data. In particular, attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly .Nodes that perform the active attacks are considered to be malicious, and referred to as *malicious nodes*, while nodes that drop the packets leaving from them, the aim of saving battery are the *selfish nodes* A selfish node changes the normal operation of the network

by not participating in the routing protocols or by not forwarding packets. Malicious node uses *the routing protocol* to announce itself as having the shorter path to the node whose data packets it needs to imprison so this type of attack called *black hole* attack. *Spoofing* is a type of attacks where a malicious node impersonates a acceptable one due to the lack of authentication in the ad hoc routing protocols. The aim of the spoofing attack is the misrepresentation of the network topology that causes network loops or partitioning. Lack of integrity and authentication in routing protocols Results fabrication *attacks* those effects in incorrect and bogus routing messages. *Denial of service (DoS)* is type of attack, where the attacker inserts a large amount of garbage packets into the network. These packets reduce a major portion of network resources, and establish wireless channel contention and network contention in the network. A *routing table overflow attack* and *sleep deprivation attack* are two other types of the DoS attack In the routing table *overflow attack*, an attacker attempts to create routes to non-existent nodes and the *sleep deprivation attack* aims to consume the batteries of an affected party node. There are also more complicated routing attacks. Compared to the simple attacks described above, these complex attacks are much harder to detect and to prevent, i.e.: *wormhole attacks* two compromised nodes create a tunnel that is linked through a private connection and thus them by-pass the network.

4. IDS FOR NODE CO-OPERATION IN MANET

Since there is no infrastructure in mobile ad hoc networks, each node must rely on other nodes for cooperation in routing and forwarding packets to the destination. Intermediate nodes might agree to forward the packets but actually drop or modify them because they are misbehaving. Only a few misbehaving nodes can degrade the performance of the entire system.

Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories:

1. **Credit-Based Schemes:** The basic idea of credit-based schemes [13] is to provide incentives for nodes to faithfully perform networking functions.
2. **Reputation-based schemes**: In this scheme [5], network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network, so that the misbehaving node will be cut off from the rest of the network. e.g Watchdog, CONFIDENT, etc. There are several proposed techniques and protocols to detect such misbehavior of nosed. In order to avoid those nodes and some schemes also propose punishment protocols [3, 4].

5. LITERATURE SURVEY

Watchdog & Pathrater proposed by S. Marti, T. J. Giuli, K. Lai, and M. Baker[5] that increases throughput in MANETs in the presence of cooperated or malfunctioning nodes. Watchdog depends upon DSR and each node takes part in the intrusion detection, on the route from source to destination, with the purpose of making sure that it has retransmitted the packet without alteration. Disadvantages of Watchdog's is that it does not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping. To moderate the effects of a misbehaving node, Marti et al. [5] introduce Pathrater, which selects a route from source to destination based on a simple rating algorithm, rather than the shortest path. Pathrater is run by each and every node in the network. Disadvantages of Pathrater is 1) inflexible binary states, 2) behavioral deceit, 3) new node anonymity, 4) reentrance of previously malicious node, and 5) encouraging selfishness and greed. Routeguard [1] similar to the Pathrater, Routeguard is run by each node in the network. However, as an improvement to Pathrater, Routeguard dispenses ratings to nodes and estimates a path metric in an improved way. Routeguard establishes a more detail and natural classification system that rates each node in the network into one of the five classes: Fresh, Member, Unstable, Suspect, or Malicious which cannot be applied directly to MANETs. Each node is treated differently based on its status and rating.

N.Nasser [6] presented intrusion detection system Ex-Watchdog, which is based on one proposed solution Watchdog. Ex-Watchdog solves a critical problem of Watchdog, Ex-Watchdog system is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, sum (total number of packets the currents node sends, forwards or receives) and path. Hence it can detect if nodes falsely report other nodes as misbehaving. The main feature of this system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and decrease the overhead significantly. Disadvantages of Ex-Watchdog are 1) it does not increase the throughput of network, 2) this system fails when malicious node is on all paths from specific source and destination.

The CONFINADT protocol proposed by Buchegger and Le Boudec [3] is similar to watchdog and Pathrater. In this protocol each node can observe the behavior of all its neighboring nodes that are within its radio range. CONFIDANT consists of four important components: The Monitor, The Reputation System, The Path Manager and the Trust Manager. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the events are passed to the Reputation System. This causes the scheme to suffer from the same problem as the watchdog scheme. It resolves one of the problems of the watchdog that it does not use the misbehaving nodes in routing and not forward packets through them, so they are punished. When a node discovers a misbehaving node, it informs all other nodes and they too do not use this node. In this scheme, every node rejects the data packets arrived from the nodes belonging to the faulty list and thus misbehaving nodes are isolated. The second mechanism is the protocol allows network nodes to send alarm messages to each other. A disadvantage of CONFIDENT is that attackers to send false alarm messages to the nodes participated in communication.

Michiardi and Molva [4] proposed a technique CORE similar to CONFIDANT which is based on monitoring and reputation system. In this method each node receives reports from other nodes. CORE allows only positive reports to pass through while CONFIDANT protocol allows the negative reports. The Denial of Service (DoS) attack is prevented as it does not allow the false report. In this system a negative rating is given when the node cannot cooperate and its reputation is decreased. When a positive report is received from this node the reputation rating is increased.

OCEAN proposed by Bansal and Baker [7] is the enhanced version of DSR protocol. In this protocol every node maintains rating for each neighboring node and monitors their behavior through promiscuous mode. Positive and negative events are recorded through the reaction of the neighbor that is expected to forward the packet. The Route Request (RREQ) message of the DSR protocol has a field named avoid-list which is use to store the faulty threshold allow nodes that misbehaved in the past to become operational by assigning a neutral rating after certain period of time. Disadvantages of OCEAN is the monitored node may not be able to relay the packet due to the low quality of wireless link, low battery, and network interface restart etc. OCEAN is not effective in reducing the throughput of misbehaving node and takes no countermeasures to prevent collusion.

Kejun liu et al [8] proposed 2ACK scheme focuses the problem of detecting misbehaving links instead of misbehaving nodes. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route. Compared with the overhearing techniques such as watchdog in [6], the 2ACK scheme solves the problems of ambiguous collisions, receiver collisions, and limited transmission power. Disadvantage of 2ACK is higher routing overhead. This additional routing overhead is caused by the transmission of 2ACK packets.

Huang and Lee [9] proposed a cluster based cooperative intrusion detection system which is capable of detection an intrusion and reveals the type of attack and attacker. This detection is possible through the statistical anomaly detection. This method uses identification rules to detect the type of attack and the attacking node. Huang and Lee used hierarchical IDS where each node has an equal chance of becoming a cluster-head. If every node involves in monitoring and analyzing the intrusion, there is a large consumption of power, hence the cluster head is responsible for computing traffic-related statistics. The energy consumption of member nodes is decreased as the cluster head overhears incoming and outgoing traffic on all members of the cluster in a one hop away. The Performance of the overall network is better; there is a decrease in CPU usage and network overhead. Disadvantages are the detection accuracy is little worse than that if the system not implementing clusters. Need to prevent a compromised node be selected as cluster head, Not mentioned about false alarm rate.

He, Wu and Kholsa [10] developed a system SORI, The Secure and Objective Reputation-based Incentive Scheme for ad hoc network focus on the packet forwarding function. It consists of three basic components: neighbor monitoring, reputation propagation and punishment. This paper, propose a Secure and Objective Reputation-based Incentive (SORI) scheme to encourage packet forwarding and discipline selfish behavior in a non-cooperative ad hoc network. The unique features of our SORI scheme are that 1) the reputation of a node is quantified by objective measures (through neighbor monitoring), 2) the propagation of reputation is secured by one-way-hash chain based authentication scheme, which is computationally efficient, and 3) the reputation of a node is only propagated to its neighbors, which greatly reduces communication overhead as compared to the schemes that maintain reputation globally. With the reputation measure obtained by the SORI scheme, we are able to design a punishment scheme to penalize selfish nodes. Disadvantages is it takes no countermeasures to prevent collusion

TWOACK: With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu et al[11] is one of the most important approaches among them. On the contrary to many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. Disadvantages are the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

AACK: Based on TWOACK, Sheltami *et al.* [12] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledges (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. Disadvantages are AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets. The functions of such detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

EAACK [14] proposed by Elhadi M. Shakshuki Malicious attackers can be detected by using Enhanced Adaptive Acknowledgement scheme. Compared to DSA, RSA has more overhead. This is acknowledging based scheme. These techniques have drawbacks due to the collusions of packets and distribution of keys between nodes becomes overhead, does not work on partial dropping attack.

Table 1.1 shows Comparison of Various Types of IDS for Node co-operation in MANET as discussed above.

6. CONCLUSIONS

Intrusion detection systems, if well designed effectively can identify malicious activities and help to offer adequate protection. Therefore, IDS has become an essential component to provide security mechanisms for MANETs. In this paper, we perform a survey on existing intrusion detection techniques in the context of MANETs. Detail description of various types of attacks on misbehaving nodes in MANET & techniques to secure MANET from different types of attacks.

REFERENCES

[1] 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.

[2] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, In Mobile Computing, Chapter 5, P153-181,Kluwer Academic Publishers, 1996.

[3] S. Buchegger and J. Le Boudec, Performance Analysis of the CONFIDANT Protocol Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, June 2002.

[4] P. Michiardi and R. Molva, Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, Communication and Multimedia Security Conference (CMS'02), September 2002.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, Proceedings of the 6th Annual International Conference , August 2000.

[6] N.Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks" in ICC 2007

[7] S.Bansal and M. Baker, "Observation Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[8] Bansal and Baker, Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs ",IEEE transactions on Mobile Computing ,P448-502, vol. 6, NO. 5, May 2007.

[9]Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proc. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003, pp. 135-147.

[10] Q.He.D.Wu and P.Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", in Proc IEEE WCN2004, Mar'04.

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Computer vol. 6, no. 5, pp. 536–550, May 2007.

[12] T.Sheltami, Al-Roubaiey, E.Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[13] L.Buttyan and J-P. Hubaux, Enforcing service availability in mobile ad-hoc WANs, Proc. of First IEEE/ACMWorkshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, August 2000.

[14] EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE

Table 1.1 Comparison of Various Types of IDS for Node co-operation in MANET

Technique	***Observation***		***Misbehaving Detection***		***Punishment***	***Avoid Misbehaving Node in route finding***	***Architecture***
	Self to neighbor	***Neighbor to neighbor***	***Selfish Routing***	***Malicious Routing***			
Watchdog/Pathrater	Yes	No	No	No	No	Yes	Distributed and Cooperative
Ex Watchdog	Yes	No	No	Yes	Yes	Yes	
CONFIDENT	Yes	No	Yes	Yes	Yes	Yes	
CORE	Yes	No	Yes	No	Yes	No	
OCEAN	Yes	Yes	Yes	No	Yes	Yes	Stand Alone
2ACK	Yes	Yes	Yes	Yes	Yes	Yes	(D&C)
Co-Operative	Yes	Yes	Yes	Yes	n/a	n/a	Hierarchical
SORI	Yes	Yes	Yes	Yes	Yes	Yes	(D&C)
TWOACK	Yes	Yes	Yes	Yes	No	Yes	(D & C)
ACK	Yes	Yes	Yes	Yes	Yes	Yes	(D &C)
EAACK	Yes	Yes	Yes	Yes	No	Yes	(D & C)