Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 7; October, 2014 pp. 15-18

http://www.krishisanskriti.org/jbaer.html

A Survey on Detection of Byzantine and Resource Consumption Attacks

Neha Mahajan[1], Rajeev Bedi[2], S. K. Gupta[3]

[1,2,3]*Department of Computer Science*
Beant College of Engineering and Technology, Gurdaspur, Punjab

Abstract: **In mobile ad hoc networks (MANETs), the primary need to achieve effective network communication among nodes is that the nodes should cooperate with each other. While in the presence of malicious nodes, this need might lead to the severe security concerns. Preventing MANET from such nodes has become an important and challenging security issue since most of the routing protocols are vulnerable to various types of attacks. In this paper we reviewed many research works which have focused on using either proactive or reactive defense mechanisms, intrusion detection systems, routing protocols to detect and prevent resource consumption and byzantine attacks.**

Keywords: **malicious attacks, byzantine attack, resource consumption attack**

1. INTRODUCTION

In MANET, nodes can communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use their intermediate node(s) to communicate with each other. All the participating nodes in this communication automatically form a wireless network, which can be observed as mobile ad hoc network [14]. Since the wireless channel is reachable to both legitimate network users and malicious attackers; there is no distinct place where traffic monitoring or access control mechanisms can be positioned so that there is no clear line of defense between the inside network and the outside world [9]. The absence of any infrastructure added with the dynamic topology of MANETs makes these networks highly susceptible to routing attacks. A malicious attacker can easily become a router and disturb network operations by violating the protocol specification since the existing routing protocols such as ADHOC on Dynamic Source Routing (DSR), Demand distance vector (AODV), Wireless MAC protocols such as (802.11) are unable to provide a trusted environment [6][14].

2. SECURITY CRITERIA'S FOR MANETS

To inspect the security state of the MANET, it is required to briefly introduce the security criteria's for a secured MANET as follows [2]:

2.1 Availability

A node should sustain its ability to deliver all the designed services irrespective of its security state. This type of security criterion are mostly challenged during denial-of-service attacks, in which all the participating nodes of the network are targeted; thus the selfish nodes make some of the services such as routing protocol or key management unavailable.

2.2. Integrity

Integrity promises the uniqueness of the messages when they are transmitted. Integrity can be categorized mainly in two ways: Malicious altering: The message can be removed, replayed or revised by a challenger, Accidental altering: The message can be lost or its content can be changed due to some benign failures; which may be transmission errors or hardware errors in communication[2][9].

2.3. Confidentiality

Confidentiality means that some information is only accessible to authorized users; the users using the network will be given different privileges in order to keep certain information secret.

2.4. Authenticity

Authenticity means an assurance that participating nodes are genuine and not impersonators. The nodes will prove their identities so as to ensure their authenticity. The failure of proving authenticity by any participant will help to protect the network from the propagation of fake messages, impersonating benign nodes and access to confidential information.

2.5. No repudiation

No repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. This can be useful to find out a node with abnormal behavior is compromised or not.

2.6. Authorization

This is generally used to assign different access rights to different level of users. This process consists of entities with

credential, which specifies the privileges and permissions it has; like the network management function can only be accessible to network administrator. The network administrator would go through an authorization process before accessing any network management functions.

2.7. Anonymity

The term anonymity is closely related to privacy preserving; which protects the privacy of the nodes from arbitrary disclosure to any other entities. All the information that can be used to recognize the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software [9][14].

3. SECURITY ATTACKS OVER MANETS AND THEIR DETECTION SCHEMES

The attacks in MANET can roughly be classified into two major categories [6]; on the basis of source of the attacks:

Passive Attacks: A passive attack acquires data exchanged in the network without disrupting the operation of the communications. Eavesdropping, traffic analysis, and monitoring are the examples of passive attacks.

Active Attacks: An active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a network. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Table 1. Security Attacks in listed layers

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping Multi-layer attacks DoS, impersonation, replay, man-in-the-middle
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

The attacks can also be classified into two categories on the basis of their domains, namely external attacks and internal attacks:

External Attacks: External attacks are carried out by nodes that do not belong to the domain of the network.

Internal Attacks: Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Attacks can also be classified according to network protocol stacks [16]. Table 1 shows the various attacks on the layers:

We will give stress on mainly two network layer attacks that is byzantine and resource consumption attacks.

3.1 Byzantine Attack

In this attack [1][12], a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

These attacks are sometimes confused with “selfish” node problem (that is, not forwarding the data packets of other nodes), but the target of nodes under two representations are different. The goal of byzantine node is to disrupt the communication of the network regardless of its own resource consumption whereas selfish nodes have a goal to reap the benefits of the other participating nodes in the network without expending its own resources in exchange. Some categories of byzantine attacks are defined below [3][16]:

3.1.1. Black Hole Attack: This is a basic type of Byzantine attack where the adversary stops forwarding data packets, drops all the packets, but still participates in the routing protocol correctly[1].

3.1.2. Byzantine Wormhole Attack: This attack is an extremely strong attack that can be performed even if only two nodes have been compromised. The malicious nodes can use the low cost form of the wormhole tunnel to increase the probability of being selected as part of the route, and then attempt to disrupt the network by dropping all of the data packets.

3.1.3 Byzantine Overlay Network Wormhole Attack: This attack is a more common variant of the previous attack which occurs when some nodes are compromised and form an overlay network. The adversaries make it give the impression to the routing protocol that they are all neighbors by tunneling through the overlay network, which considerably increases their probabilities of being selected on routes.

3.1.4. Flood Rushing Attack: This attack takes place during the broadcast of a legitimate flood and can be elaborated as a

competition between the legitimate flood and the adversarial variant of it. If an adversary positively influences some of its neighbors with its own version of the flood packet before they obtain a version through a legitimate route, then those neighbor nodes will ignore the legitimate version and will propagate the adversarial version. This may affect the ability to establish an adversarial-free route, even in the presence of certain authentication techniques [16].

3.2 Resource Consumption Attack

This attack is commonly known as the sleep deprivation attack. An attacker tries to consume or waste away resources of other nodes present in the network [7][8]. The attacks could be in the form of unnecessary route requests (RREQ) for routes, very regular generation of beacon packets, or forwarding of stale packets to other nodes. [12]The resources are directed with the three aspects that are bandwidth, computational power, and battery power which are always only limitedly available in ad-hoc networks. The attacker keeps the node busy by pumping the packets to that node and consumes it's all battery power; which takes the form of sleep deprivation attack. Most of the solutions for detecting with detection of malicious node deal with two major categories i.e. Proactive and reactive schemes [6]:

Proactive Detection Schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage.

Reactive Detection Schemes are those that trigger only when the destination node detects a significant drop in the packet delivery ratio. In these schemes the resources are not wasted as compared to proactive schemes.

4. RELATED WORK

We have summarized the following schemes available for detecting resource consumption and byzantine attacks along with the advantages and disadvantages and the approaches used by each of them.

Table 2. Listing existing schemes

SCHEME/ METHOD	APPROACH	MERITS	DEMERITS
Self-Organizing Scheme[11]	Four algorithms were performed by each nodes to detect malicious behaving leader in a leader based network	1.Protects the normal behaving leader to be declared as node 2. No constraints on leader selection algorithm, which makes it applicable to any leader based network	Mechanism can only be applied to leader based networks
Dendritic Cell Inspired Intrusion Detection Algorithm[8]	DCIIDA is used to protect the network from intrusions using packet verifiers, antigen extractors and signal extractor	Artificial Intelligence System properties such as being self-healing, self-defensive and self-organizing has meet the challenges of securing the MANET environment	1. It is required to reduce the possible false positive rates
Channel Aware Detection Algorithm[3]	Identified the selective forwarding misbehavior due to normal loss events such as medium access collision or bad channel quality	Considered a challenging scenario, normal channel loss events Analytical studies to determine optimal detection threshold that minimizes the summation of false alarms and missed detection thresholds	It gives large overhead in the presence of the attackers.
Hash function based method[13]	The method was used to generate node behavioral proofs that contain information from both data traffic and forwarding paths to detect collaborative packet drop attack	It introduced limited computational overhead Investigated the security and design schemes to further improve the efficiency and reduce overhead	Other collaborative attacks needs to be investigated Routing protocol integration may give a comprehensive scheme
New Semantic	The approach	Robust in	Proposed

SCHEME/ METHOD	APPROACH	MERITS	DEMERITS
Algorithm[5]	was able to identify and prevent four routing attacks parallely: packet eavesdropping, Message tampering, Black hole and gray hole	nature since it is able to identify and prevent four routing attacks parallely	approach has shown high throughput as compared to AODV and DSR
Cooperative Detection Mechanism[10]	Firstly the malicious node is detected then the neighbor nodes of that initiates the cooperative detection mechanism	Malicious node detection rate is high Overhead detection rate is low	Other attacks need to be investigated for integration
Mean Field Game Theoretic Approach[15]	Modeled the interactions among a malicious node and a number of legitimate node	Powerful mathematical tool for problems with a large number of players	The average lifetime and the compromising probability can be improved

5. CONCLUSION & FUTURE WORK

It has been analyzed that during the presence of the set of compromising nodes which misbehaves and participates in the exploitation of the network communication; it becomes very difficult to detect resource consumption and byzantine attacks. The techniques mentioned above to detect these attacks are based on either proactive or reactive architecture. The intrusion detection systems used usually gives the problem of false alarms. We consider this as severe security problem and our future work will involve the detection of both attacks using a hybrid approach which will not give the problem of false alarming. The Qos parameters such as packet delivery ratio, throughput, end-to-end delay and routing overhead would be used to compare their performances.

REFERENCES

[1] Abhay Kumar Rai, Rajiv RanjanTewari and Saurabh Kant Upadhyay(2010), Different Types of Attacks on Integrated MANET-Internet Communication, *International Journal of Computer Science and Security (IJCSS)* Volume 4: Issue 3

[2] AdityaBakshi, A.K.Sharma and Atul Mishra(2013), Significance of Mobile AD-HOC Networks (MANETS), *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Volume-2, Issue-4

[3] DevuManikantanShila, Student Member, IEEE, Yu Cheng, Senior Member, IEEE, and Tricha Anjali, Senior Member, IEEE (2010), Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMN, *IEEE Transactions on wireless communications*, Vol. 9, No. 5

[4] Dilip Vishwakarma, Deepak Chopra(2012), An Efficient Attack Detection System for Mobile Ad-hoc Network, *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume-1, Issue-6

[5] G. S. Mamatha and Dr. S. C. Sharma (2010), A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS, *International Journal of Computer Science and Security*, Volume 4: Issue 3

[6] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai (2014), Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait DetectionApproach, *Systems Journal, IEEE* , Volume: PP, Issue: 99 , January 2014.

[7] MahaAbdelhaq, RaedAlsaqour, Mohammed Al-Hubaishi, Tariq Alahdal, and MueenUddin (2013), The Impact of Resource Consumption Attack on Mobile Ad- hoc Network Routing, *International Journal of Network Security*

[8] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail and Daud Israf, "Detecting Resource Consumption Attack over MANET using an Artificial Immune Algorithm", Research Journal of Applied Sciences, Engineering and Technology 3(9): 1026-1033, 2011 ISSN: 2040-7467 © Maxwell Scientific Organization, 2011

[9] PradeepRai and Shubha Singh (2010), A Review of 'MANET's Security Aspects and Challenges', *IJCA International Journal of Computer Applications Special Issue on "Mobile Ad-hoc Networks" MANETs*

[10] ReenaSahoo and D.r P.M Khilar (2011), Detecting Malicious Nodes in MANET based on a Cooperative Approach, International Journal of Computer Applications

[11] Seyed Mohammad AsghariPari, Mohammad Noormohammadpour, Mohammad JavadSalehi (2013), A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks approach, *Wireless Days (WD), 2013 IFIP, IEEE*

[12] ShabirSofi, Eshan Malik, Rayees Baba, Hilal Baba and Roohie Mir (2012), Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation, Communication and Information technology (ICCIT)

[13] Weichao Wang, Bharat Bhargava and Mark Linderman (2009), Defending against Collaborative Packet Drop Attacks on MANETs, *2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS)*

[14] Wenjia Li and Anupam Joshi (2011), Security Issues in Mobile Ad Hoc Networks - A Survey, *International Journal of computer applications*

[15] Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE (2014), A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks, *Wireless Communication, IEEE Transactions on (Volume: 13, Issue-3)*

[16] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei(2006), A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, *Wireless/Mobile Network Security, Springer*