IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Review on Various Kinds of Attacks in MANET

[1] Munish Wadhwa; [2] Ashwani Sethi

[1] Department of Computer Engineering
Guru Kashi University
Talwandi Sabo Bathinda,Punjab(151001) India.

[2] Department of Computer Engineering
Guru Kashi University
Talwandi Sabo Bathinda,Punjab(151001) India.

Abstract - As MANET is a infrastructure less network where various wireless nodes without any central controller sends and receives the data. As it is infrastructure less network. Is highly vulnerable to various kinds of attacks. For making network to be safer for communication there requires various levels of protocols level protective measures. So that the performance of the network can be safeguarded.

Keywords - *MANET,Attacks,Sybil,Black hole,Gray Hole*

1. Introduction

1.1 Security in MANET

Security: The aims of Ad hoc networks and mainly MANET have in recent years not only seen general use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's collection from simple wireless home and office networking to sensor networks and similarly constrained deliberate network environments. Security aspects play an important role in almost all of these application situations given in the wireless network.

Protecting Mobile ad hoc networks: In the ad hoc networks, nodes do not start out aware with the topology of their networks instead, they have to discover it. The basic idea is that a new node may declare its presence and should listen for messages broadcast by its neighbours. Each node learns about neighboring node and how to reach them.

Reactive approach: This type of protocols keeps new lists of destinations and their routes by periodically distributing routing tables in the network.

Proactive approach: In proactive routing protocols the method is different than the reactive routing protocols. In this type of protocols essentially routes are depends upon the traffic control which is continuous. All routing information preserved at any time of the network because we know that network is dynamic which changes its size by making its size increasing or decreasing.

1.2 Security Goals

- **Confidentiality:** it ensure that message should be kept secret between sender and receiver. Message should protect form passive attack such as eavesdropping and traffic analysis.
- **Integrity :** it ensure that message is not modified in transit in any unauthorized manner, it deals with authenticity of data. Integrity should protect form active attack such as man-in-middle attack.
- **Availability :** it deals with service and resource of network to authentic members.it should protect form attack such as denial of service attack.
- **Authentication :** it provide a trusted membership to users in network and verify and validate identity of user with a pre-shared secret (password) or digital certificate.
- **Authorization :** it limit access level of users in network, which user can access particular services.
- **Resilience :** it is survivability of network if a network segment is compromised, network should resist attack with help of mitigation technique and sustain network operation and services.
- **Timely Delivery :** this term also known as data freshness, attacker can send previously capture data and repeat this data for time critical application require real time data such as data analysis ,remote site monitoring ,war field sensing this application required accurate data.

1.3 Attacks in MANET

- **Denial of Service attack:** This attack aims to attack the availability of a node or the whole network. The attack

is effective the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion technique.

- **Impersonation:** If the confirmation mechanism is not properly implemented a malicious node can act as an honest node and monitor the network traffic. It can also send false routing packets, and gain access to some private information.
- **Black hole Attack:** In this attack, an attacker uses the routing protocol to present itself as having the shortest path to the node whose packets it wants to intercept.
- **Wormhole Attack:** In wormhole attack, a malicious node receives packets at one location in the network and passages them to another location in the network, where these packets are resent into the network. This passageway between two colluding attackers is referred to as a wormhole.
- **Replay Attack:** A replay attack is a form of network attack in which a valid data transmission is maliciously or delayed. This is agreed out either by the originator or by an adversary who stops the data and retransmits it.
- **Man- in- the- middle attack:** An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases attacker may imitate the sender to communicate with receiver or imitate the receiver to reply to the sender.
- **Eavesdropping:** This is a passive attack. The node simply observes the trusted information. This information can be later used by the malicious node. The secret information like location, public key, private key and password can be drawn by eavesdropper.
- **Snooping:** Snooping is illegal access to another person's data. It is similar to eavesdrop but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.
- **Sybil Attack:** Sybil is named after the woman identified as multiple personality disorder. Sybil attack is implemented when a malicious node claim multiple fabricated or stolen identity and effect the network operations. Sybil attack is damaging the security and trust of network in peer to peer and distributed network. Sybil node gain disproportional amount of resource in network using multiple identities.

2. Literature Survey

[1] N.Venkatadri (2016) et al: Ad Hoc wireless network is a type of wireless network, in which there is no any fixed infrastructure. Devices in Ad Hoc network can move around the network within a given range. Currently most of the transactions are performed through the computer networks so they are more susceptible to many physical security threats. One of the major DOS Attacks that degrade the performance of the whole MANET is Black Hole attack. In the presence of black hole attack, nasty nodes are not forward the packets rather they drop packets. In this work, black hole attack is detected and eliminated through implementing Digital Signature with Twofish Algorithm. We modified on-demand routing protocol Temporally Ordered Routing Algorithm (TORA) and named it as STORA. Our proposed STORA performs well under normal conditions and under black hole attack than original TORA.

[2] Pham Thi Ngoc Diep(2015) et al: Delay Tolerant Network (DTN) is developed to cope with intermittent connectivity and long delay in wireless networks. Due to the limited connectivity, DTN is vulnerable to blackhole and greyhole attacks in which malicious nodes drop all or part of the received packets intentionally. Although existing proposals could detect the attack launched by individuals, they fail to tackle malicious nodes cooperating to cheat the defense system. In this paper, we suggest a scheme to address both individual and collusion attacks. Nodes are required to exchange records of previous encounters and evaluate others based on their messages forwarding ratios. Malicious nodes might avoid being detected by colluding to hide misbehaving forwarding ratio metrics. To persistently drop packets and promote the metrics at the same time, attackers need to create forged encounter records at high frequency and with high number of sent messages. This leads to abnormal patterns of fake encounters in contrast ith authentic ones and provides a symptom for collusion detection. Extensive simulation shows that our solution can work with various dropping probabilities and different number of attackers per collusion at high accuracy and low false positive.

[3] Harsh Pratap Singh,2013) et al: Mobile ad hoc network is an assembly of mobile nodes that haphazardly forms the temporary network and it is an infrastructure less network. Due to its self-motivate or mobility in nature the nodes are more vulnerable to security threats which stimulate the performance of the network. In this paper, a review on a various types of coordinated attack is deliberated such as blackhole / grayhole attack which are most serious threats in mobile ad hoc network. In cooperative blackhole attack more than one node collude to each other hence this attack is more challenging to identify. This paper presents a review of different security mechanism to eliminate the blackhole / grayhole attack from the network.

[4] Yanzhi Ren,(2014) et al: The Delay Tolerant Networks (DTNs) are especially useful in providing mission critical services including emergency scenarios

and battlefield applications. However, DTNs are vulnerable to wormhole attacks, in which a malicious node records the packets at one location and tunnels them to another colluding node, which replays them locally into the network. Wormhole attacks are a severe threat to the normal network operation in DTNs. In this article, we describe various methods that have been developed to detect wormhole attacks. However, most of them cannot work efficiently in DTNs. To detect the presence of a wormhole attack, we propose a detection mechanism that exploits the existence of a forbidden topology in the network. We evaluated our approach through extensive simulations using both Random Way Point and Zebranet mobility models. Our results show that the proposed method can detect wormhole attacks efficiently and effectively In DTNs.

[5] Kanu Geete(2014) et al: A wireless mesh network is a kind of multi-hop network and can be used as synonym for an ad-hoc network. It is a network having many to many connections with the capability of dynamically healing the network topology. Security is a challenging application of a wireless mesh network. The self configurable self organized nature makes a wireless mesh network more vulnerable to various types of attacks. Exploitation of a WMN can cause a large scale degradation of network performance. In this paper we have discussed some attacks that are performed on various layers of TCP/IP model. And we performed a comparative study for a specific network layer attack: grey hole attack. A grey hole attack is often difficult to detect and recover. There are different techniques for its detection which have their advantages and shortcomings.

[6] Yinghui Guo(2014) et al: Future VANET Vision: Ubiquitous deployment of VANET/VDTN capable systems from different vendors • Can not centralize security infrastructure Big attack surface (even for closed systems) • Proposed systems mostly realized using widely available commodity hard- and software • WiFi Technology • Off-the-shelf operating systems and hardware platforms

3. Problem Definition

As in existing paper they have addressed the problem of grey and black hole attacks in wireless sensor network. As in this type of network malicious node can drop the messages rather than forward the messages. It will decrease the network performance as large amount of the packets being dropped. They have used the technique to enquire from the neighbor nodes to check there message received versus forward messages for their previous communication. Any malicious node avoids this information to provide. Because it will definitely effects the identity of the malicious nodes. But the problem is even malicious node can provides the wrong information about the packet forward ratio.

4. Proposed Work

In Current Research a technique of sharing hash value amongst the nodes before communication. So that the legitimate nodes has the legal hash value. Any malicious node does not has the ability to share the hash value. Because that is only known to the legitimate nodes.
So once the new technique will be applied the both techniques can be compared on the basis of different parameters like packet delivery ratio. Throughput and end to end delay Etc.

5. Conclusion

It is clear that the network of MANET nature can have performance deterioration if certain node behaves in malicious way. As there is no central controller in the network , which can control the access of the malicious node. Without increasing the hardware cost protocol level improvement is required so that network performance can be enhanced.

Future Work

While considering the identification of the malicious node there must be certain way to control the access of malicious node in the network.

References

[1] N.Venkatadri, Reham Abdellatif Abouuhogail and Ahmed Yahya, “Secure TORA: Removal of Black Hole Attack using Twofish Algorithm”, International Journal of Software Engineering and its Applications, 2016.

[2] Pham Thi Ngoc Diep, Monika Sachdeva, “Detecting Colluding Blackhole and Greyhole ttack in Delay Tolerant Networks”, ICRTEDC-2015, Vol. 1, Special Issue. 2.

[3] Jaydip Sen ,” Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” , Bengal Intelligent Park, Salt Lake Electronic Complex, Kolkata, INDIA,2014

[4] Bansi S. Kantariya1, Dr. Narendra M. Shekokar2,” Detection and Mitigation of Greyhole Attack in Wireless Sensors Network Using Trust Mechanism”, (2013)

[5] Pham Thi Ngoc Diep,” Detecting Colluding Blackhole and Greyhole Attack in Delay Tolerant Networks”,2015.

[6] Yanzhi Ren,” Detecting Wormhole Attacks in Delay Tolerant Networks”,2015

[7] Harsh Pratap Singh," Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", Volume 64– No.3, February 2013

[8] Kanu Geete," A Survey on Grey Hole Attack in Wireless mesh Networks", Volume 95– No.23, June 2014

[9] Akinlemi Olushola O, K. Suresh Babu, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[10] Madjid Merabti, David Llewellyn-Joes, and Kashif Kifayat, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[11] Ashima Singla and Ratika Sachdeva, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[12] R. Kanni Selvam , Mr.C.Karthikeyan, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

[13] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.

[14] Hegde.S, Uvaraj Arutkumaran.S, "An efficientMesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[15] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.