ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Analysis on Security Threats and Mitigation Techniques in Wireless Mesh Network

Shilpa[1], Kamaljeet Kaur Mangat[2]

M.Tech Student, Dept. of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab, India[1]

Assistant Professor, Dept. of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab, India[2]

ABSTRACT: Wireless mesh network(WMN) has emerged as a key solution for upcoming technologies. It is possible because of the auto configuration and self healing nature of these networks. However the capability of wireless mesh network provide an ease for network deployment , easy maintenance, low cost, high scalability, flexible integration but on the other hand it make it prone to various security attacks . This paper reviews security threats faced by WMN along with various methods to mitigate certain attacks such as black hole attack, warm hole attack in order to secure WMN .

KEYWORDS: Wireless Mesh Network ,Security Attacks ,PASER,IBC-HWMP,SHWMP etc.

I. Introduction

Wireless mesh network is most widely used in information technology .Wireless mesh networks(WMNs) have facilitated the emergence of airborne network assisted applications[1].WMNs are dynamically self configured and self organized thus establish an ad-hoc network inevitably and maintain linkage between nodes[2].WMNs consist of mesh routers (i.e. nodes) and mesh clients(i.e. users).Mesh routers form the backbone of wireless network and mesh clients connect directly to the routers [3].Mesh clients make access to the network through mesh routers .They can directly connect i.e. mesh with each other[4]. The progress of this technology has to deal with the demanding security, architecture and protocol design issues. Security issues are highly important in concern to wireless mesh network for their exploitation.

Security attacks are often classified into two types based on operation of the network. It can be classified as active and passive attack. In active attack assailant disrupts the network whereas in passive attack attacker steals the information from the communication[5].Denial of service is one of the major attack on wireless mesh network. It is a type of attack in which authorized user are denied service in the requested time[2].

Black hole attack is a type of DOS attack. A black hole attack is also known as sink attack .It occurs when a specific node i.e. malicious node defines itself to be most optimal node to forward packet but drops the packet forwarded by neighbouring nodes. Fig 1. Depicts the effects of black hole attack where data is directed towards malicious node. In this attack, the malicious node invariably replies absolutely to a RREQ ,although it’s going to not have a main route to the destination. Because the malicious node doesn’t make certain its routing entries, it will be the key to reply to the RREQ message. Therefore, the entire traffic in the neighbourhood of the malicious node are directed towards it, that drop all the packets ,leading to denial of service[5].

Grey hole attack is another variant of black hole attack. The opponent node avoids the detection by dropping the packet selectively. This can be a describe as a result of malicious node forwarding packet only by selection. It doesn’t describes the complete denial of service but it go unseen for a larger amount of time. It may be considered as congestion within the network[2].

DOI: 10.15680/IJIRCCE.2016. 0406168

In Sybil attack ,a malicious node pretends the characteristics of many nodes ,each viewing as a legitimate node with aim to disrupt the network traditional operation .This attack degrades the routing performance and additionally disrupts the routing services[3].

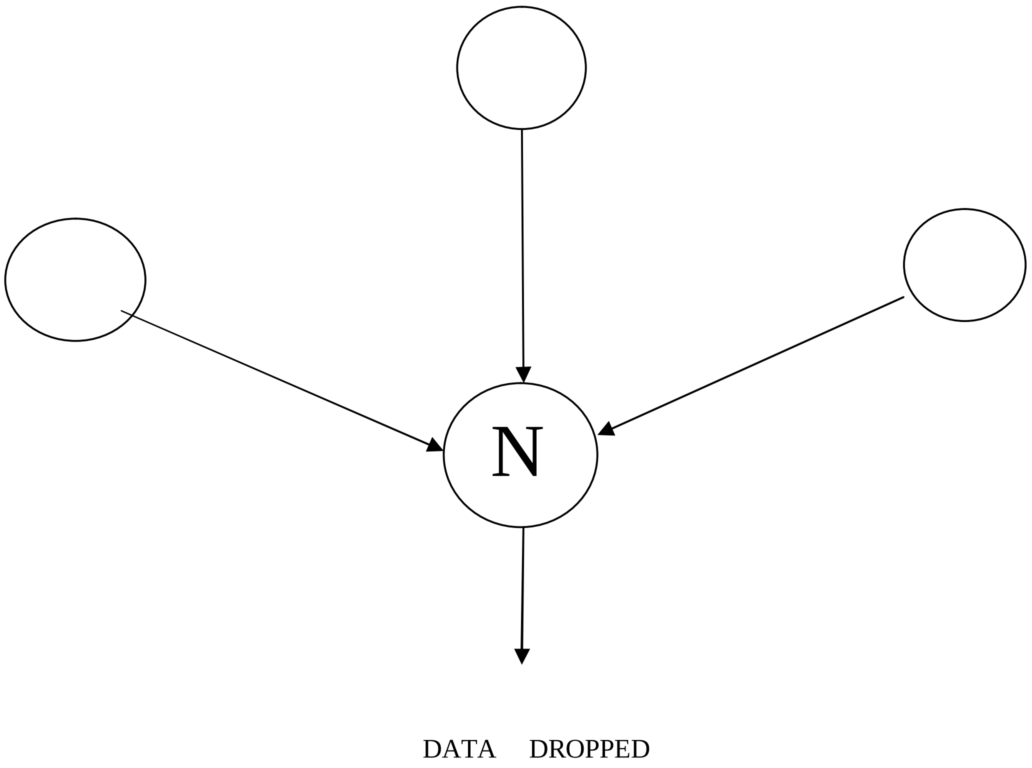

Figure .1 Illustration of black hole effect

II .RELATED WORK

Mitigation techniques are used to protect the wireless mesh network from the various attacks. In order to alleviate the security problems in wireless mesh network several countermeasures for wireless mesh network have been put forward. In this section we will discuss the countermeasures for wireless mesh networks.

Mohamad Sbeiti(et al.)[1] proposed PASER (Position Aware Secure and Efficient Routing) approach that uses a hybrid cryptosystem approach with efficiently securing the routing process. The authors attempt for a deployable secure routing solution. Firstly it make use of asymmetric cryptography for initial mutual authentication and key exchange. Then it make use of the symmetric cryptography to authenticate routing messages. PASER incorporates an in-band key management technique to tackle the interdependency cycle problem among secure routing protocols and key distribution strategies. PASER combats a good range of routing attacks because it aims to meet all the security requirements.

Ben-Othman and Benitez [6], [7] present an Identity Based Cryptography (IBC) mechanism to raise the protection level of the existing HWMP. The authors propose two modifications trust management for internal nodes and digital signature of routing messages with IBC for external nodes. The employment of the IBC eliminates the need to verify the authenticity of public keys and ensures the integrity of the management message in HWMP. Simulation results show that the IBCHWMP doesn’t induce an comprehensive overhead compare to the original HWMP protocol.

Islam et al. [8] propose the Secure HWMP (SHWMP), to produce authenticity and integrity of HWMP routing messages and stop unauthorized manipulation of changeable fields within the routing information parts as shown in fig2.To attain this, they use the Merkle tree idea to authenticate changeable information and symmetric key cryptography to shield the mutable field. Simulation results illustrate that the SHWMP give high packet delivery ratio with small increased end-to-end delay, path acquisition delay, in addition to control byte overhead. Though, the proposed protocol is prone to the attacks caused by the inner legitimate mesh routers.

IN [9] ,authors focused on the black hole and grey hole attack and apply the OLSR(Optimized link state routing protocol and analysis of these attacks and their effects on networks. To thwart the network layer from these attack during which false node act as regular node. That node is too hard to find, as a result during this kind of attack, malicious node are very much erratic and unstable as they varies from normal to opponent and opponent to normal nodes. It is found that black hole attack is at ease to identify than grey hole attack.

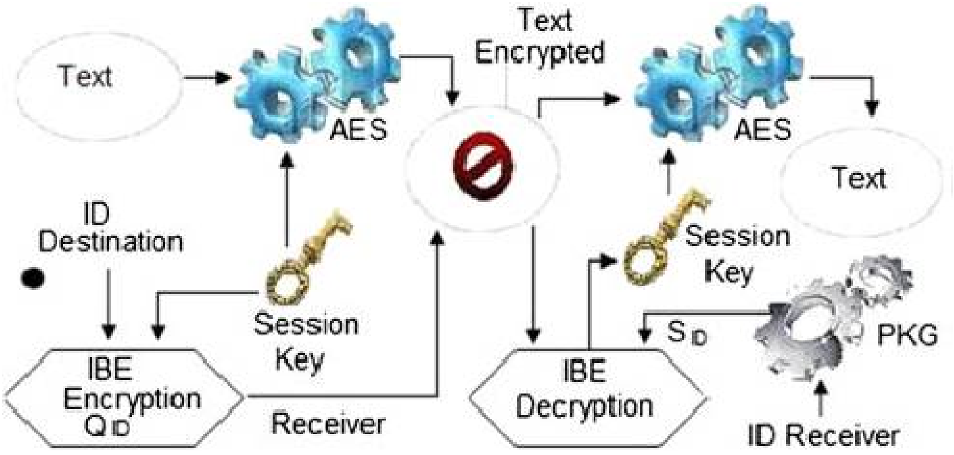

Figure. 2. Encryption and decryption using the identity-based encryption(IBE),AES,Advanced Encryption standard;PKG,private key generator.

Oliviero and Romano [10] propose an extension of the Ad-hoc On-demand Distance Vector (AODV), named AODV-DEX, so as to shield AODV against gray hole or sinkhole attacks. The main plan is to switch the hop count values so as to allow them to reflect information regarding the nodes' reputations on a path. To attain this goal, two reputation levels are considered the global reputation: a global reputation equipped by other nodes through the dissemination protocol and the native information (i.e., a local reputation, coming from the observations provided by the watchdogs). These two levels are integrated to outline the reputation that can be exploited to judge the real behaviour of a node. Simulation results show that the employment of the reputation metric in AODV will boost both the security level and also the performance of the network, even within the presence of routing attacks.

S.NO	AUTHOR NAME AND YEAR	PROBLEM ADDRESSED	PROPOSED SOLUTION	RESULTS	OUR REVIEW
1.	Mohamad sbeiti[2016]	It aims on the security of the routing functionality in UAV-WMN.	PASER : a secure route discovery approach for wireless mesh network	The route discovery approach PASER is able to prevent the network from routing attacks	Proposed approach is able to shield the network from routing attacks.
2.	Rupinder kaur and Parminder singh[2014]	Black hole and grey hole attack in wireless mesh Network	OLSR(Optimized link state routing protocol)	It prevent network against effects of black hole and grey hole attack and find black hole is easy to detect than grey hole attack	OLSR protocol prevent some of the attack but cannot provide protection of attacks at network layer.
3.	Ben-Othman and Benitez[2011]	Security mechanism for hwmp to prevent against routing attacks	IBC-HWMP	Reduces the long overhead involved in HWMP..	The approach has implementation concerns making it more prone to the attacks
4.	S. Islam,A. Hamid and C.S. Hong[2009]	HWMP(hybrid wireless mesh protocol) is vulnerable to attacks such as route disruption and diversion, spoofing etc.	SHWMP(Secure hybrid wireless mesh protocol	It prevents all the identified attacks and prevents unauthorized manipulation of fields.	The proposed protocol is likely to the attacks caused by the inner valid mesh routers.
5.	Oliviero and Romano[2008]	Gray hole or sinkhole attack	AODV-DEX	It increases the security level of network and prevent against grey hole or sinkhole attack	It improves the performance of network even in the presence of routing attacks.

Table. 1. Comparison of different mitigation techniques.

III. Conclusion and Future Work

WMN is a standard technology for providing IP services due to its quick and easy deployment. However due to its characteristics such as open medium it makes it prone to attacks. Security is one of the main challenging issue of WMN.

In this paper we discussed about the attacks on wireless mesh network. Under this survey ,we have evaluated the effectiveness of several defence mechanisms to protect the wireless mesh network against attacks(such as black hole attack ,warm hole attack ,grey hole attack) .The IBC-HWMP uses elliptic curve cryptography. Many researchers have implementation concerns with this approach .Thus making it prone to security attacks. The PASER(Position Aware Secure and Efficient Routing) has been found the best mechanism to protect against attacks on WMNs. This approach uses hybrid cryptosystem over existing approaches to provide additional security to wireless mesh network.

Although security in wireless mesh network has attracted many researchers. In future scope, the implementation of the existing defence approaches can be used in broader range of application scenarios. Thus it will make wireless mesh network more resistant to security attacks.

REFERENCES.

1. Sbeiti Mohamad, Niklas Goddemeier, Daniel Behnke, and Christian Wietfeld,"PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks.", *IEEE Transactions on Wireless Communications*, vol.15, no. 3 ,pp. 1950-1964,2016.
2. S. Singh and I. Kaur, "Security against Active Attacks in Wireless Mesh Networks.", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 66-67, 2012.
3. Sgora, Aggeliki, Dimitrios D. Vergados, and P. Chatzimisios. "A survey on security and privacy issues in wireless mesh networks.", *Security and Communication Networks*, 2013.
4. Lin, Hui, Jianfeng Ma, Jia Hu, and Kai Yang. "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11 s wireless mesh networks.", *EURASIP Journal on Wireless Communications and Networking* , no. 1 ,pp. 1-16,2012.
5. Aswal, M. S., Paramjeet Rawat, and Tarun Kumar. "Threats and vulnerabilities in wireless mesh networks.", *International Journal of Recent Trends in Engineering,* vol.2, no. 4, 2009.
6. Ben-Othman, Jalel, and Yesica I. Saavedra Benitez. "On securing hwmp using ibc." In *2011 IEEE International Conference on Communications (ICC)*, pp. 1-5, 2011.
7. Ben-Othman, Jalel, and Yesica I. Saavedra Benitez. ,"IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11 s.", Concurrency *and Computation: Practice and Experience* 25, no. 5 (2013): 686-700.
8. Islam, Md Shariful, Md Abdul Hamid, and Choong Seon Hong, "SHWMP: a secure hybrid wireless mesh protocol for IEEE 802.11 s wireless mesh networks.",In *Transactions on Computational Science VI*,Springer Berlin Heidelberg,pp. 95-114,2009.
9. Kaur Rupinder, and Parminder Singh, "Black hole and grey hole attack in wireless mesh network", American journal of engineering research,vol.3,no.10,pp. 41-47,2014
10. Oliviero, Francesco, and Simon Pietro Romano,"A reputation-based metric for secure routing in wireless mesh networks." In the Proceedings of 2008 IEEE Global Communications Conference (GLOBECOM 2008), New Orleans, LO, USA, pp. 1-5, December 2008.

DOI: 10.15680/IJIRCCE.2016. 0406168