© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

The Survey of Various Types of Wireless Sensor Network and Paser Protocol

Paramjit Kaur [1], Rakesh Kumar[2] and Harinder Kaur[3]

[1]Research (Scholar), Department of CSE, SECG, Gharuan, Punjab, India
[2]Dean and Associate Professor, SECG, Gharuan, Punjab, India
[3]Assistant Professor, Department of CSE, SECG, Gharuan, Punjab, India

ABSTRACT

Mesh wireless network is an advanced developing technology that will modify the world more efficiently or effectively. It is regarded as a highly capable field being adding significant in mobile wireless networks of the future group. Low-altitude Unmanned Aerial Vehicles combined with WLAN Mesh Networks have facilitated the emergence of airborne network-assisted applications [1]. In misadventure release, they are key solutions for (i) on-demur ubiquitous network access or (ii) efficient investigation of sized areas. However, these solutions still face major security experiments as WMNs are prepared to routing attacks. In this paper, we studied the benefits of WMN and also describe the different types of attacks of WSN. We discussed about PASER Position Aware Secure and Efficient Mesh Routing and its process in mesh network.

Keywords : Mesh system, PASER, Control plane attack, Rushing Attack, Wormhole Attack, Black hole Attack.

I. INTRODUCTION

Wireless mesh networks (WMNs) are increasingly recognized as ideal solutions to ubiquitous last-mile high-speed Internet access. A typical WMN has a layered structure, as shown in Figure 1. The first layer consists of access points (APs) which are high-speed wired Internet entry points. At the second layer, stationary mesh routers form a multihop backbone via long-range high-speed wireless techniques such as WiMAX [1]. The wireless backbone connects to wire APs at some mesh routers through high-speed wireless links. It provides multihop wireless black hole between wired APs and mesh clients (i.e., end users) at the lowest layer1 Mesh clients, while at rest or in motion, can assess the network either by a direct wireless link to a nearby mesh router or by a chain of other clients to a mesh router out of reach[2,3].

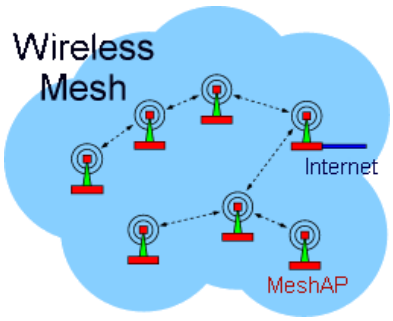

Figure 1: Wireless Mesh Network [15]

Wireless mesh stemming can allow people living in distant zones or minor industries working in pastoral districts to join their systems assigned for reasonable Internet networks. Mesh system is a system topology in which every node relays data for the system. All mesh nodes co-operate in the portion of data in [6] the system. A mesh system whose nodes are all coupled to each other is a fully connected system. Fully connected systems have the compensation of security or reliability and difficulties in a wired node affects only the two mesh nodes attached to it [7].

II. METHODS AND MATERIAL

1. PRIOR WORK

Liet al. (2006) [8] described mesh network is vulnerable to privacy attacks because of the open medium property of wireless channel, the fixed topology, and the limited network size. Traditional anonymous routing algorithm cannot be directly applied to Mesh network, because they do not defend global attackers. In this paper we design private routing algorithm that used "Onion", i.e., layered encryption, to hide routing information. In addition, we explore special ring topology that fits the investigated network scenario, to preserve a certain level of privacy against a global adversary.

Zhou et al. (2012) [9] described to complete high-capacity performance. The numeral of mesh routers and the number of accesses necessity is accurately chosen. It too exposes that a WMN can accomplish the same asymptotic output capacity as that of a hybrid ad hoc network by indicating only a small number of interlocks routers.

Lin et al. (2012) [10] defined a PA-SHWMP, which combines new dynamic standing mechanism based on subject logic and uncertainty with the multi-level security technology. PA-SHWMP can defend to the internal attacks caused by compromised nodes and accomplish stronger security and privacy protection.

Sgora et al. (2013]) [11] presented Wireless Mesh Networks are considered as a promising solution for offering low-cost access to broadband services. However, one of the main challenges in the design of these networks is their vulnerability to security attacks. In this paper, we analyze the fundamental security challenges and constraints of these networks, classify several possible attacks, and survey several intrusion prevent, detect, and response mechanisms found in the literature.

Sarma et al. (2014) [12] presented systemMANET is an infrastructure less, dynamic, de-centralized network. Any node can join the network and leave the network at any point of time. Due to its simplicity and flexibility, it is widely used in military communication, emergency communication, academic purpose and mobile conferencing. In MANET there is no infrastructure hence each node acts as a host and router. They are connected to each other by Peer-to-peer network. De-centralized means there is nothing like client and server. Each and every node is acted like a client and a server. Due to the dynamic nature of mobile Ad-HOC network it is more vulnerable to attack. Since any node can join or leave the network without any permission the security issues are more challenging than other type of networks. One of the major security problems in ad hoc networks is called the black hole problem. It occurs when a malicious node referred as black hole joins the network. The black hole conducts its malicious behavior during the process of route discovery. For any received RREQ, the black hole claims having route and propagates a faked RREP. The source node responds to these faked RREPs and sends its data through the received routes. Once the data is received by the black hole, it is dropped instead of being sent to the desired destination.

2. APPLICATION OF WIRELESS MESH NETWORK

WMNs introduce the concept of a peer-to-peer mesh topology with wireless communication between mesh routers. This concept helps to overcome many of today's deployment challenges, such as the installation of extensive Ethernet cabling, and enables new deployment models. Deployment scenarios that are particularly well-suited for WMNs include the following:

- Campus environments (enterprises and universities), manufacturing, shopping centers, airports, sporting venues, and special events.
- Military operations, disaster recovery, temporary installations, and public safety.
- Municipalities, including downtown cores, residential areas, and parks.
- Carrier-managed service in public areas or residential communities. Due to the recent research advances in WMNs, they have been used in numerous applications. The mesh topology of the WMNs provides many alternative paths for any pair of source and destination nodes, resulting in quick re-configuration of the path when there is apath failure. WMNs provide the most economical

data transfer coupled with freedom of mobility. Mesh routers can be placed anywhere such as on the rooftop of a home or on a lamppost to provide connectivity to mobile/static clients. Mesh routers can be added incrementally to improve the coverage area.

III. RESULTS AND DISCUSSION

1. PASER (POSITION AWARE SECURE AND EFFICIENT MESH ROUTING)

PASER's main target scenarios are disaster rescue and relief operations. In such environments, safeguards are indirectly applied to the nodes preventing their compromise, like nodes are mounted on fire brigades tubes. Thus, internal attacks, where nodes from within the network are involved a less realistic threat in these environments, whereas external attacks, which are performed by illegitimated nodes, are of paramount importance.

1) Mainly efficient and secure

- *Efficient Secure Routing*:Symmetric cryptosystem use the secret key to encrypt and decrypt a message and asymmetric cryptosystem use public key to encrypt and private key to decrypt a message.
- *Set of Routing's Band Key Management:* To resolve the inter-dependency cycle between key management and secure routing.

2) Security Aims

- Message confirmation, message cleanness, neighbor verification and dynamic key management.
- Prevent external hackers from changing and routing process.
- Enthusiastically eliminate inputs or nodes/ update keys.
- Difficulties are less in internal hackers [2].

2. TYPE OF ATTACKS IN WIRELESS MESH NETWORK

- Control plane attack

These are the major attack in the WMN as the attackers make the routes unavailable or control the routing path. The attacker just targets the steering functionality for system level. The examples of attack are rushing attack, black hole, worm hole and so on [14].

- Rushing Attack

It is launched by a malicious node that forwards the route request message before any other intermediate node by ignoring the specified delay.

- Worm Hole Attack

In worm hole attack, there are malicious nodes are collected by starting a tunnel by an efficient message standard. Wormhole assaults can be masterminded effectively. For making a wormhole assault, no less than two handsets are situated at distinctive areas on a remote system by assailant.

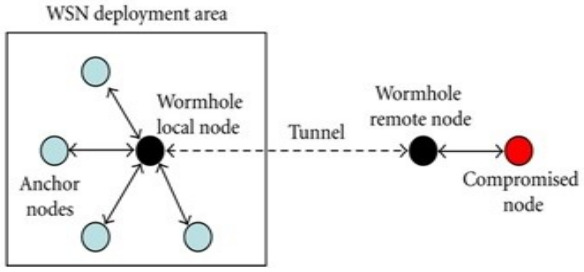

Figure 2. Wormhole attack [16]

- Attack of Black Hole

The hateful node always replies definitely to a route application although it may not have an effective route to the endpoint. Almost all the traffic within the neighborhood will be directed toward the malicious node, which may drop all the packets.

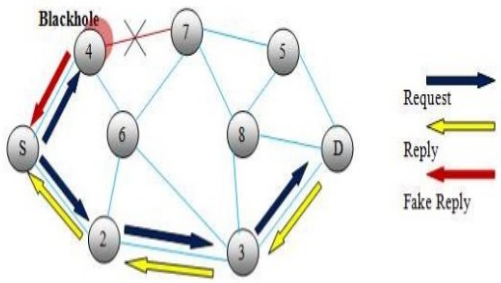

Figure 3. Black hole attacks [17]

- Data level attacks

This attack is launched by these selfish nodes or the malicious node which is been compromised by the attacker by dipping packets or vaccinating the hateful data into the network. This may lead to the DDoS attack in the system. So the main impartial of the attacker is to

cause the DDoS to legitimate userby creating data undeliverable.

IV. CONCLUSION

In this paper, we have discussed the main security issues and challenges in Wireless Mesh Networks. We concluded the security attacks in various routes, while most attacks are much harder to counter because the challenger is aware of the network secrets and protocols. These adversaries are detected by behavioral metrics such as per-packet status. However, these metrics cannot detect attacks of selective nature, where high-value packets are targeted. An attacker drops only few packets, due to congestion or poor wireless congestion.

V. REFERENCES

[1]. Eugen,B.(2009),"Wireless Mesh Networks Technologies: Architectures, Protocols, Resource Management and Applications." University POLITEHNICA Bucharest. Electronics, Telecommunication and Information Technology Faculty. Prancis, Vol 2, No. 4.

[2]. Baldini, B., Allen, D. and Vergari, F. (2014), "Survey of Wireless Communication Technologies for Public Safety," IEEE Communications Surveys Tutorials, vol. 16, no. 2.

[3]. Liu, S., Jia, S. and Sun, TY. (2008),"Research on optimization efficiency of Genetic Algorithms." Systems and Control in Aerospace and Astronautics, 2008. ISSCAA 2008. 2nd International Symposium on. IEEE, 2008.

[4]. Mark, C. and Spafford, G. (1995), "Applying Genetic Programming to Intrusion Detection." In Proceedings of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8. Cambridge, Massachusetts.

[5]. George,A. (2008),"Wireless Mesh Networking. McGraw-Hill Professional, vol. 24, No. 10.

[6]. Kerpez, KJ. (1997),"Coaxial cable passive mesh networks. "Communications, IEEE Transactions on 45.8 (1997): 937-947.

[7]. Zhang, Y. and Fang, Y. (2006), "ARSA: An Attack-Resilient Security Architecture for Multi hop Wireless Mesh Networks," IEEE Journal on Selected Areas in Communications, vol. 24, No. 10.

[8]. Xiaoxin, W. and Li, N. (2006)"Achieving privacy in mesh networks."Proceedings of the fourth ACM workshop on Security of ad hoc or sensor networks. ACM, 2006.

[9]. Ping, Z., Wang, X. and Rao, R. (2012),"Asymptotic capacity of infrastructure wireless meshes networks." Mobile Computing, IEEE Transactions, vol.7, pp. 1011-1024.

[10]. Hui, L., Ma, J. and Hu, J. (2012),"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.

[11]. Aggeliki, S. and Chatzimisios, P. (2013),"A survey on security or privacy issues in wireless mesh network ks." Security or Communication Networks.

[12]. Sarma, KJ., Sharma, R. and Das, R. (2014)," A Survey of Black Hole Attack Detection in Manet", Advanced Information Networ king or Applications (AINA), 2014 24th IEEE International Conference on. IEEE, 2014.

[13]. Cheikhrouhou, O. andChaouchi, H. (2006), "Security architecture in a multi-hop mesh network", In Proc. 5th Conference on Security and Network Architectures.

[14]. Banerjee, S., Sardar, M. and Majumder, K. (2014),"Black-hole attack mitigation in manet", springer international publishing switzerlor.

[15]. http://www.surfability.com/ITC/mesh.php.

[16]. http://networksimulator2.com/ns2-wormhole-attack.

[17]. http://www.slideshare.net/Kunal1194/study-of-security-attacks-in-manet.