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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Survey on PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks

[1]Nikhil Dhule, [2]Prof. G.T. Chavan,

Department of Computer Engineering Sinhgad College of Engineering Pune. Savitribai Phule Pune University

Maharashtra, India [1, 2].

ABSTRACT: Recent advances in embedded systems, energy storage, and communication interfaces, accompanied by the falling prices of WLAN routers and a considerable increase in the throughput of a WLAN (IEEE 802.11), have facilitated the proliferation of WLAN Mesh Network (WMN) applications. In addition to their current deployments in less dynamic community networks, WMNs have become a key solution in various highly dynamic scenarios. For instance, WMNs are intended to interconnect self-organized, cooperative, and small Unmanned Aerial Vehicles in a wide range of applications, such as emergency response, environmental monitoring, and ad-hoc network provisioning. Wireless mesh network has served as backbone for establishment of several upcoming technologies. It is possible owning to self-healing, auto configuration nature of these networks. On one hand it offers an ease for compatibility, availability, feasibility however on other hand these networks are prone to various security attacks. These security attacks can sabotage the communication between sender and receiver. A need of algorithm that can prevent the network from security attacks such as DoS attack. The proposed work we implements a position-aware, secure, and efficient mesh routing approach (PASER). Our proposal prevents more attacks than the IEEE 802.11s/i security mechanisms and the well-known, secure routing protocol ARAN, without making restrictive assumptions. A hybrid cryptography algorithm will provide additional security mechanism to the system.

KEYWORDS: Processor, Speed, RAM, Hard Disk, Key Board.

I. INTRODUCTION

In practice there is increase in humanitarian disasters and economic damages. The example of earthquake and tsunami in Japan, 1.9 million fixed telephone lines and 29000 cellular base stations were damaged. Thus disaster areas like Japan there is an emergence of restoration of whole communication network in minimum time with more efficiency over large scale. But practically it is not possible. Full restoration of communication network takes more time. The UAVs acts as a WLAN or LTE aerial hotspots to achieve this requirements. UAV helps in coverage extension and weather monitoring. To get connect UAV immediately with ground control station the internet and cellular network also needed. For this easy deployment of UAVs the airborne mesh network is used. WMN provides self-healing and auto-configuring characteristics.

System analyzes the route discovery delay of the protocols in theory and in simulation. We derive lower bound equations of this delay as it constitutes along with the routing overhead, for which we provide asymptotic expressions, the main impact on the overall network performance. The results show that PASER has a more efficient and robust route discovery process than ARAN and BATMANS, and it is scalable with respect to network size and traffic load.

Using the network simulator NS, realistic UAV-mobility patterns, and an experimentally derived channel model, we investigate the performance of the protocols in representative UAV-WMN scenarios under multiple traffic types and various scenario sizes. The results show that PASER mitigates in UAV-WMN more attacks than its alternatives. On top of that, PASER achieves performance comparable to that of HWMPS. This combination of values (security and performance) is deemed to be necessary by the IETF Keying and Authentication for Routing Protocols (KARP) group to drive a broad deployment of a secure routing protocol.

DOI: 10.15680/IJIRCCE.2017. 0504308

This system proposed PASER secure routing approach in UAV- WMN. Here, discussed attacks in ad-hoc network and security aspects in PASER. PASER reduces in the different case more attacks than the well-known secure routing protocol and the standardized security mechanisms of IEEE 802.11s/i. It can be used at broad range.

II. OBJECTIVE

To achieve its secure routing objectives, PASER seeks to fulfill the following security goals, which are cryptographic goals and can thus be realized using cryptographic techniques (for detailed information about cryptographic goals and information security goals.

- **Message authentication:** Assuring the party that receives a message that the party which sent the message is an authorized node, and that the message has not been altered by unauthorized nodes during transport.
- **Message freshness:** Assuring the party that receives a message that the message is fresh. That is, it has not been received before.
- **Neighbor authentication:** Assuring one party the identity of a second party involved, and that the second is located in its transmission range.
- **Origin authentication:** Assuring the party that receives a message the identity of the message originator.
- **Dynamic key management:** Providing a dynamic method to distribute and revoke network keys, and to exclude nodes. Due to the distribution of encrypted symmetric network keys (GTK/CTK) as well as the certificate revocation list (CRL).

III. LITERATURE SURVEY

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.

Mohammad 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 makes use of asymmetric cryptography for initial mutual authentication and key exchange. Then it makes 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. 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 neighboring nodes. System 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 neighborhood 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 describe the complete denial of service but it goes unseen for a larger amount of time. It may be considered as congestion within the network [2].

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 a 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 whole attack.

Olivier 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 behavior 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.

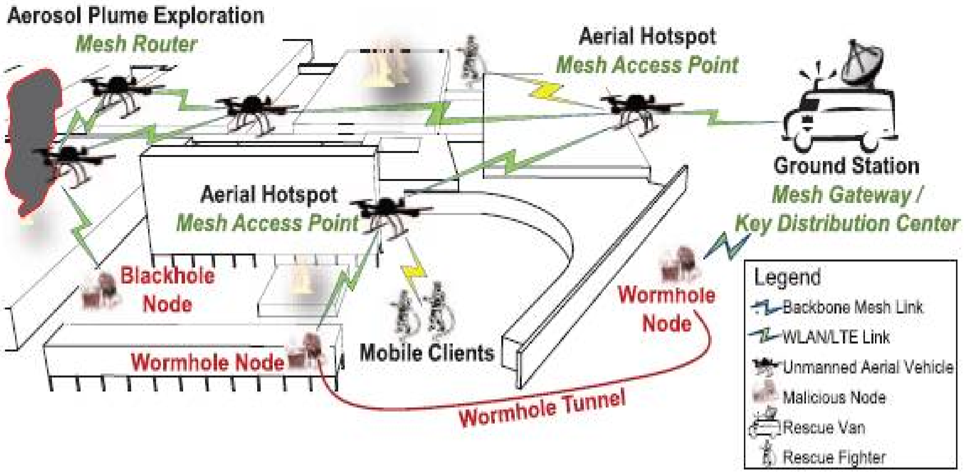
System	**Algorithms for security**	IEEE Standards
PASER	RSA + SHA1	IEEE 802.11i/s
Hybrid Wireless Mesh Protocol	IBC	IEEE 802.11s
BATMANS	Lattice base cryptography	IEEE 802.11i
ARAN	Blowfish for security	IEEE Journal on Selected Areas in Communications,
Proposed system	RSA + AES128	MAC standard IEEE 802.11

DOI: 10.15680/IJIRCCE.2017. 0504308

SECURITY COMPARISON - COMPARISON OF MITIGATED ATTACK

Attacker Type	Attack name	Security goals	PASER	ARAN	HWMPS	BATMANS
External	Internal attacks	Message authentication	Disabled	Disabled	Disabled	Disabled
	Time-based replay	Message freshness	Disabled	Disabled	Disabled	Disabled
	Position-based replay	Neighbor authentication	Disabled	Possible	Possible	Possible
	MAC impersonation	MAC address authentication	Possible	Possible	Possible	Possible
	Wormhole	Neighbor authentication	Disabled	Possible	Possible	Possible
		MAC address authentication				
Internal	Flooding and path deviation	Intrusion detection and dynamic key management	Prevent	Depends	Possible	Possible
	IP impersonation	IP address authentication	Depends	Depends	Possible	Possible
	Fabrication	Origin authentication	Disabled	Disabled	Possible	Possible
		Intrusion detection and dynamic key management				
	Black hole	Intrusion detection and dynamic key management	Depends	Depends	Possible	Possible
		IP address authentication	Prevent	Depends		

IV. SYSTEM (ARCHITECTURE) AND WORKING



System architecture

The WMN capability for auto-configuration and self-healing significantly reduces the complexity of network deployment and maintenance; it makes the WMN backbone prone to routing attacks, which include the black hole and wormhole attacks. As a result, the attacker can, with little cost and effort, redirect the traffic and drop the data packets even if the wireless backbone links are encrypted. In UAV-WMN-assisted disaster relief situations, this can sabotage the communication between rescue fighters. In addition, the command and control data exchanged between the UAVs and their ground station will get disrupted. This issue makes the use of WMNs (or any wireless multi-hop solution relying an a routing protocol to dynamically set up routes) problematic for the command and control of UAVs in practice, as flight regulations impose that it should be always possible to remotely pilot the UAVs. Because the UAVs are highly dynamic, relying on the exchange of information for autonomous cooperative positioning [God12a], the attacker might also alter their flight paths by selectively dropping packets. In case the attacker is able to compromise network credentials and as long as there is no efficient way to refresh those credentials, the attacker might manipulate payload data or even inject corrupted control information that could lead to the high jacking of an UAV. For instance, the attacker might impersonate an UAV and propagate corrupted position information, exploiting the UAVs' collision avoidance mechanisms to indirectly steer UAVs to areas controlled by the attacker. Since the disruption of communications and the violation of the flight security of UAVs can lead to fatal consequences (e.g., near airports), it is vital to deploy a secure UAV-WMN backbone.

IV. CONCLUSION

WMN is now a day's providing an extensive support for IP services and upcoming technologies. Security is one of the challenging issues still exist in wireless mesh network. There is a high need to protect the network from attacks and making it furthermore reliable to form the backbone of many existing infrastructure. The work done in this paper shows the elimination of malicious nodes with the help of Hash RSA algorithm. The simulation of the network was done in NS2 with the effect during the DoS attack. We identified the malicious nodes and then black listed them during the routing. Hybrid cryptography was used in improving the key generation process of the Hash RSA algorithm. The results show significant improvement with the use of Hash RSA optimized with hybrid cryptography. The performance was analyzed and checked on various parameters like throughput, jitter and end to end delay. The performance of Hash RSA optimized with hybrid cryptography is validated under different scenarios in terms of variable number of nodes. Throughput of algorithm increases with increase in number of nodes. Whereas end to end delay varied less in nature. The slight increase is due to congestion in network. Jitter value increases by increase in nodes. The high negative value portrays jitter has improved .Due to congestion in network there is slight variation in delay of packet. The algorithm performs better in terms of all parameters. It provides much greater performance and handles the security of network.

For future enhancement Security feature in network has attracted many researchers. In the future scope the implementation of algorithm can be applied in various application scenarios such as to relay the communication between UAV, deployment of IP services. Thus it will help in making wireless network furthermore reliable.

REFERENCES

[1]. SbeitiMohamad, NiklasGoddemeier, 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.

[4]. Aswal, M. S., ParamjeetRawat, and Tarun Kumar. "Threats and vulnerabilities in wireless mesh networks.", International Journal of Recent Trends in Engineering, vol.2, no. 4, 2009.

[5]. 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.

[6]. 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.

[7]. Islam, MdShariful, Md Abdul Hamid, and ChoongSeon 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.

[8]. KaurRupinder, 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

[9]. Oliviero, Francesco, and Simon PietroRomano,"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.