Authentication and security models in Wireless Mesh Networks: A Survey

Cintre Simmi, Research scholar, Department of Computer Science and Engineering, Rayalaseema university, Andhra Pradesh, India.

M. Nagabhushana Rao, Professor,Department of Computer Science and Engineering, Ramachandra college of engineering, Eluru, Andhra Pradesh, India.

Abstract— Security is a key parameter in supporting data communication over wireless mesh networks(WMNs). Due to high computational time, memory, traffic and bandwidth, several routes in the WMNs are not secured for data communication. Mesh routers are always stationary and essential for constructing the network backbone. On the other hand, the network coverage must be enhanced along with high scalability. The most important characteristic of WMN is to relay the information that are transmitted from different nodes. As wireless routers are interconnected through wireless links and mesh clients, it is extremely difficult to find the malicious packets or attacks in the network during the data communication. In this paper, we survey authentication and security models in WMNs. Also, the issues and challenges of the traditional authentication and security models are studied in this paper.

Keywords— Mesh networks, Authentication, Data security, Encryption, Attacks

I. INTRODUCTION

Wireless mesh network (WMNs) can be defined as the basic radio frequency based networks. This network contains different numbers of mesh routers and mesh clients. The mesh routers are also known as routing devices or access points. Mesh routers are stationary in nature and these are responsible for building the backbone of the network. Mesh clients have restricted amount of energy than that of mesh routers. Mobility, flexibility and robustness can be achieved with the help of WMNs. Apart from this, the network coverage can also be enhanced with high scalability. The applications of wireless mesh networks include healthcare, enterprise networking, security surveillance, etc.

Two types of attacks are possible in WMNSs, those are active and passive attacks. Both passive as well as active attacks in WMNs communicate through wireless multi-hop process. In case of wireless mesh networks, passive attacks may violate confidentiality. On

the other hand, active attacks may violate authentication, integrity and non-repudiation. Hence, it is essential to develop an efficient and effective security scheme to exchange the information during communication. To achieve mutual trust and secure communication in between different mesh devices, a new key establishment service is developed [1]. Most of the traditional approaches [2][3] are inefficient due to energy, storage and bandwidth constraints. Therefore, there is necessity of an advanced authentication technique in order to overcome all the issues of wireless mesh networks.

Distributed network architecture, shared multi-hop wireless backbone and dynamic modification of network topology are the factors that influence the WMNs. All of the authentication schemes in WMNs can be classified into two categories, those are:-

1. Home-foreign-based technique
2. Broker-based technique

In case of a home-foreign-based model, every individual mesh client is registered with its home network for a long period. Mutual authentication can be achieved via interactions among the mesh client's home network and foreign network. Apart from this, the round trip may cause authentication delay that may affect different real time applications such as voice over IP. Again, the authentication signaling overhead increases with increase of clients' base.

According to the broker based architecture, mutual authentication among mesh client and wireless mesh network can be carried out without the influence of client's home network. It can decrease the handover and authentication latency in order to support real time services. The long term operator authentication latency exists if the mesh client is handed over from a single operator network to a different one. In order to achieve most effective and efficient authentication strategy, the following requirements are considered:-

1. Mutual authentication approach must be implemented among mesh client and that particular wireless mesh network in order to access more reliable connection.
2. The authentication delay of inter-operator and intra-operator handover is required to be very low in order to restrict service interruption.
3. Localized authentication must be implemented in order to lighten the loads of authentication servers.
4. The authentication method must be integrated with an advanced key agreement approach in order to ensure the protection of communications in between entities.

5. Several attacks such as key spoofing and replay attacks can be discarded with the help of these security authentication technique.
6. The privacy must be preserved at the time of authentication in order to discard every individual unauthorized entity. It also considers the mesh client's actual identity and present location.

In recent years, with the increase in data size and communication channel, data of the data in the WMNs also increases exponentially. The main objective of WMNs is to ensure the data integrity and confidentiality against the third party attacks. Therefore, the data security in WMNs is not only related to network monitoring but also associated with data integrity and data encryption. The traditional cryptosystem framework based on public key infrastructure (PKI) can achieve data security, confidentiality and non-repudiation along with limitations. In order to encrypt data, the third party provider needs to obtain the authorized sensor's public keys and then communicate the cipher data to the individual authorized sensor, which increases the bandwidth and processing overhead.

Traditional cryptographic models are categorized into two types; those are symmetric security models and asymmetric security models. The most useful symmetric encryption approaches in WMNs are AES, DES, RSA, Blowfish and elliptical curve cryptography. AES, DES and ECC can be used to improve the security under asymmetric security models. But, traditional asymmetric approaches use different keys for data encryption and decryption process.

RELATED WORKS

J. Sun, et.al, introduced a new security architecture in order to achieve anonymity and traceability in case of wireless mesh networks [1]. The process of anonymity adds protection for users in order to access network services without being visible. Apart from this, the network authority needs conditional anonymity such as misbehaving entities in the network. In this work, they presented an advanced security architecture in order to satisfy unconditional anonymity in case of authorized users. Again, the above presented technique has the responsibility to trace each and every misbehaving entity for the network authorities in case of wireless mesh networks.

K. Chi, et.al, emphasized on fast handoff in case of secure IEEE 802.11s mesh networks [2]. IEEE 802.1X authenticato us used to decrease the additional computation cost of

IEEE 802.1X authentication processes at the time of handoff. Also, this technique can be implemented in the generic multi-hop wireless networks.

X. Lin, et.al, introduced an advanced compromise-resilient authentication architecture for wireless mesh networks [3]. User authentication process has significant importance in case of service oriented communication networks. These systems have the responsibility to detect and discard all kinds of unauthorised network access. A secure wireless network must have appropriate authentication mechanism, authorisation and accounting framework. In the above scenario, either a single or multiple identical and duplicate AAA servers are present.

T. Gao, et.al, introduced an anonymous authentication technique that completely depends upon identity-based proxy group signature for wireless mesh network [4]. Access security is considered as the major challenge during the communication of wireless mesh network. In this work, they used a new proxy group signature technique that completely depends upon the identity. This technique is integrated with proxy group signature and identity-based group signature technique. They have considered the hierarchical proxy architecture of wireless mesh networks.

D. K. Altop, et.al, proposed a secure and efficient distributed key establishment protocol for wireless mesh networks [5]. In this paper, they have introduced an effective and efficient security establishment protocol which can be implemented in case of wireless mesh networks. The above-mentioned protocol completely depends upon identity-based key establishment. There is no trusted authority involved during the process of private key generation. This process is not applicable to large numbers of mesh nodes.

T. Gao, et.al, presented an advanced localized efficient authentication technique in case of multi-operator wireless mesh networks along with identity-based proxy signature scheme [6]. Proposed model construct secure access and communications in case of a multi-operator wireless mesh network. Mutual authentication can be established among mesh clients and access mesh router with the help of a ticket. The bilinear pairing based key agreement function is merged along with the proposed technique in order to protect the communications in between various entities.

A. Gaur, et.al, proposed a polynomial based technique in order to establish authentic association in case of wireless mesh networks [7]. In this work, they proposed a polynomial based technique which is responsible for providing pairwise connectivity, low communication, average storage overhead and higher scalability.

A. Hassanzadeh, et.al, proposed a traffic- agnostic intrusion detection system for resource-constrained wireless mesh networks [8]. Intrusion detection is considered as the most common and vital security mechanism in case of wireless mesh networks. In this work, a practical traffic aware detection system is introduced for resource-constrained wireless mesh networks. In this proposed technique, a new coverage technique is also introduced to monitor and manage local and backbone wireless mesh network traffic.

C. Hsu, et.al proposed a linear multi-secret sharing technique in order to carry out group communications in wireless mesh networks [9]. Presently, WMNs are considered as the most important technology that includes low cost community wireless services. Secure group communication is considered as the most vital component in wireless mesh networks.

Y. Lai, et.al, developed a new ticket-based authentication technique in order to achieve fast handoff in WMNs[10]. This technique completely depends on mesh ticket authentication. Various sensitive information such as time and date of expiration are transmitted in plain text. Hence, the chances of security risks become high. This protocol involves high quality tamper proof devices. This technique results high level of security along with extended privacy. This approach is better as compared to other traditional approaches in terms of authentication delay.

S. Lee et.al, emphasized on the design and implementation of an advanced data protection technique with the help of OTP in a wireless network [11]. One time password is the most commonly used authentication technique. This technique uses a randomly produced nonce. The prime objective of this method is to resolve the security issues which usually occur when same password is used for all of the transactions. In this above proposed method, a nonce is used as an encryption key during the process of encryption. At the time of data exchange, a new random number is produced. Therefore, this method extends the boundaries of security mechanism.

References

[1] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks", "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011", pp. 295-308.

[2] K. Chi, Y. Shih, H. Liu, J. Wang, S. Tsao and C. Tseng, Fast Handoff in Secure IEEE 802.11s Mesh Networks, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 60, NO. 1, JANUARY 2011, pp. 219-233.

[3] X. Lin, R. Lu, P. Ho, X. Shen, and Z. Cao, TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 7, NO. 4, APRIL 2008, pp. 295-308 389-1400.

[4] T. Gao, F. Peng and N. Guo, Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network, Journal on Wireless Communications and Networking (2016) 2016:193.

[5] D. K. Altop, Md. A. Bing¬ ol, A. Levi and E. Savas, DKEM: Secure and EfÞcient Distributed Key Establishment Protocol for Wireless Mesh Networks, Ad Hoc Networks.,

[6] T. Gao, N. Guo, K. Yim, LEAS: Localized efficient authentication scheme for multi-operator wireless mesh network with identity-based proxy signature, Mathematical and computer modelling.

[7] A. Gaur, A. Prakash, S. Joshi, D. P. Agrawal, Polynomial based scheme (PBS) for establishing Authentic Associations in Wireless Mesh Networks, J. Parallel Distrib. Comput. 70 (2010), pp. 338-343.

[8] A. Hassanzadeh, R. Stoleru, M. Polychronakis and G. Xie, RAPID: Traffic-agnostic intrusion detection for resource-constrained wireless mesh networks, Computer and security (2017), pp. 1 -17.

[9] C. Hsu, G. Cui, Q. Cheng and J. Chen, A novel linear multi-secret sharing scheme for group communication in wireless mesh networks, Journal of Network and Computer Applications 34(2011), pp. 464–468.

[10] Y. Lai, P. Cheng, C. Lee and C. Ku, A New Ticket-Based Authentication Mechanism for Fast Handover in Mesh Network.

[11] S. Lee, B. Kang, K. Cho, D. Kang, K. Jang, L. Parka, and S. Parka, Design and Implementation for Data Protection of Energy IoT utilizing OTP in the Wireless Mesh Network, 4th International Conference on Power and Energy Systems Engineering, CPESE 2017, 25-29, September 2017, Berlin, Germany