Wireless Local Area Network (WLAN): An Enhanced Authentication System Using Key Authentication Based Secured Multicasting (KABSM)

Gattu Sandeep
Assoc. Prof.
Department of ECE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

Ramesh Bhanothu
Asst. Professor
Department of ECE
Siddhartha Institute of Technology and Sciences
Narapally, Hyderabad, Telangana, India

***Abstract* - Multicasting is a quick and easy technique to send the same data to numerous users on the network at the same time, cutting down on transmission time. Because multicasting involves broadcasting to a large number of individuals, there is a risk of developing a vulnerability to various attacks. MKMP - Multicast Key Management protocol is utilized in the existing system, which sends session information about users to substations for distinct groups. The user list under the sub stations is difficult to comprehend, and there is a risk of missing or mismatching the user list with the station information. To address this issue, the KABSM-[Key Authentication based Secured Multicasting] solution is presented in this study, which gives a citizenship key for enabling all network node functions such as entering a region, communicating, and so on. In this method, a dynamic key is generated and allocated to the entire network's nodes. The simulation results suggest that the proposed strategy is more efficient than the existing method.**

Keywords: WLAN, Key Management, Multicast Key Management, Secured Multicasting.

1. INTRODUCTION

There are two types of LANs that enable connection for interconnecting computing resources at the local levels of an organization. Wired LANs vs. Wireless LANs, Wired LANs vs. Wireless LANs, Wired LANs vs. Wireless LANs, Wired LANs vs. Wireless LANs, Wired LANs Flexibility, portability, mobility, and ease of installation are all advantages of wireless LANs. For good reason, Wi-Fi (wireless fidelity)-based wireless local area networks (WLANs) are one of today's fastest expanding technologies in businesses, schools, and households. They let users to stay connected when away from their offices by providing mobile access to the Internet and workplace networks. When there is no wired Ethernet infrastructure available, these networks can be up and operated rapidly. Without relying on skilled corporate installers, they may be put to work with minimal effort. WLANs have a number of corporate benefits, including:

- Continuously mobile workers are connected to their critical applications and data
- New applications based on continuous mobile connectivity can be deployed
- Intermittently mobile workers can be more productive if they have continuous access to email, instant messaging, and other applications
- Immediate interconnections among arbitrary numbers of participants become possible.
- Instead of authenticating a user, the 802.11 protocol relies on authenticating a wireless station or device. There are two types of authentication in the specification: open authentication and shared key authentication. The following transactions make up the 802.11 client authentication process.
- An enquiry request frame is broadcast on every channel by the client, and access points within range react with a probe response frame.
- The client selects the best access point (AP) for access and sends an authentication request
- The access point responds with an authentication response
- After successful authentication, the client sends an association request frame to the access point
- The access point responds with an association response

- The client is now able to send traffic to the access point

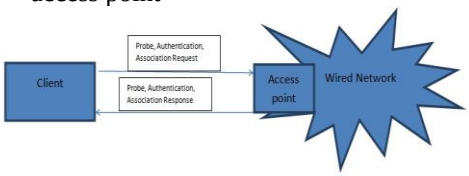

Figure-1: WLAN communication

2. RELATED WORKS

The author of this paper shows how to identify the root cause of inefficiency. The author then offers FLAP [1], an efficient authentication technique, to overcome this flaw. The author of this work created and executed a large-scale WLAN monitoring system. The authors discuss their methodology, scalability, management viewpoints, designs, and solutions [2]. The design, implementation, and assessment of a channel, robust, accurate, and low-overhead Device-free-passive localization system are presented in this study [3]. The authors suggest a privacy-preserving proximity-based security solution for location-based services in wireless networks in this research [4], which does not require any pre-shared secrets, trusted authorities, or public key infrastructure. The authors of this study concentrate on a denial-of-service attack. It's also known as a keyhole attack or selective forwarding. The author developed a FADE strategy to solve this problem. Using forwarding evaluations and two-hop acknowledgement monitoring, Forwarding Assessment-based Detection identifies sophisticated assaults. [5].

The author of this paper discusses the Extensible Authentication Protocol. This protocol is a widely used authentication framework in Wireless Local Area Networks. EAP methods are authentication procedures based on the Extensible Authentication Protocol. [6]. The author of this paper identifies the various issues associated with roaming services as a set of voluntary and necessary needs. Then they give a quick rundown of current work's state of the art. Finally, they provide a problem that must be solved in roaming authentication [7]. The author offers a unique PHY-CRAM for WLAN in this study. Both one-way and mutual authentication are possible using the physical layer Challenge-Response Authentication Mechanism. The orthogonal frequency-division multiplexing approach is used by PHY-CRAM. In various threats and channel conditions, PHY-CRAM achieves both a low false acceptance rate and a high successful authentication rate [8]. Using physical layer security concepts, the author presents a strategy for permitting an automatic bootstrap and periodic renewal of the network key in this study. The scrambling of groups of consecutive packets is the basis of this approach. It isn't necessary to utilise an initial authentication [9]. The authors of this work recommend that spatial information, a physical attribute connected with each node that is difficult to falsify and independent of encryption, be used instead [10]. The author offers the Hand-auth mechanism in this work. When compared to other protocols, this protocol has good computation and efficiency. [11].

Proposed Approach

Figure-2 depicts a network with N number of users who have registered and deployed in the network. During node registration, the Base Station assigns each node a key for secure communication, and key creation is depicted in Equation-[1]. Nodes must provide their citizenship key and have it confirmed whenever they want to communicate. If the key is invalid, the node will be flagged as a malicious node and will be removed from the network.

$$KEY_{node-i} = [random(N) + Node_{ID}] \neq KEY_{node-1\ to\ N} \quad \text{----}$$

Equation-[1].

The KEY is a network-wide unique value that cannot be replicated or misappropriated by any other node. In KABSM, a data packet from a source node is multicast to a n number of nodes in the network by grouping the destinations by ID, and the group nodes then submit their key to the sub-stations and are authenticated. The multicoated data packets can be received once the nodes have been authenticated.

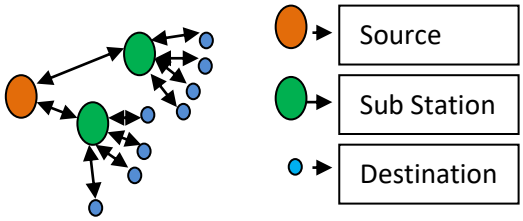

Figure-2: Multicasting

3. RESULTS AND DISCUSSION

In terms of Delay, Throughput, and Energy, the output of the network simulator for KABSM is compared to the MKMP technique. In terms of throughput, the proposed approach outperformed the previous strategy in terms of transmission. The proposed method sent 56000 packets in parallel, which is higher than the current system. The communication delay should be kept to a minimum and the packet transmission operations should be maximized. In terms of energy efficiency, the new method outperformed the previous method. The

proposed solution saves 88 percent of energy by increasing the number of packets in parallel over the current system.

4.CONCLUSION

This work concluded that the suggested technique outperforms the present approach in terms of detection rate, energy, and throughput. When comparing energy and throughput, the proposed approach outperforms MKMP. Finally, the performance and throughput of the KABSM method is obtained. Citizenship key-based communications are used to maximize security levels at each and every communication establishment step. As a result, the proposed approach is more reliable and performs better than existing approaches.

REFERENCES

[1]. Xinghua Li ; FenyeBao ; Shuxin Li ; Jianfeng Ma, "FLAP: An Efficient WLAN Initial Access Authentication Protocol", Parallel and Distributed Systems, IEEE Transactions on (Volume:25 , Issue: 2), Feb. 2014

[2].Tan, K. ; McDonald, C. ; Vance, B. ; Arackaparambil, C. ; Bratus, S. ; Kotz, D., "From MAP to DIST: The Evolution of a Large-Scale WLAN Monitoring System", Mobile Computing, IEEE Transactions on (Volume:13 , Issue: 1), Jan. 2014

[3]. Saeed, A. ; Kosba, A.E. ;Youssef, M., "Ichnaea: A Low-Overhead Robust WLAN Device-Free Passive Localization System", Selected Topics in Signal Processing, IEEE Journal of (Volume:8 , Issue: 1), Feb. 2014

[4]. Xiao, L. ; Yan, Q. ; Lou, W. ; Chen, G. ; Hou, Y.T., "Proximity-Based Security Techniques for Mobile Users in Wireless Networks", Information Forensics and Security, IEEE Transactions on (Volume:8 , Issue: 12), Dec. 2013

[5].Qiang Liu ; Jianping Yin ; Leung, V.C.M. ; ZhipingCai, "FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs", Wireless Communications, IEEE Transactions on (Volume:12 , Issue: 10), October 2013

[6].Chun-I Fan ; Yi-Hui Lin ; Ruei-Hau Hsu, "Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs", Parallel and Distributed Systems, IEEE Transactions on (Volume:24 , Issue: 4), April 2013

[7].Daojing He ; Chun Chen ; Jiajun Bu ; Chan, S. ; Yan Zhang, "Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects", Communications Magazine, IEEE (Volume:51 , Issue: 2), February 2013

[8].Shan,D.;Kai Zeng ; Weidong Xiang ; Richardson, P. ; Yan Dong, "PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks", Selected Areas in Communications, IEEE Journal on (Volume:31 , Issue: 9), September 2013

[9]. Baldi, M. ; Bianchi, M. ; Maturo, N. ; Chiaraluce, F., "A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks", Wireless Communications Letters, IEEE (Volume:2 , Issue: 2), April 2013

[10]. Jie Yang ; Yingying Chen ; Trappe, W. ; Cheng, J., "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", Parallel and Distributed Systems, IEEE Transactions on (Volume:24 , Issue: 1), Jan. 2013

[11]. DaojingHe ;Jiajun Bu ; Chan, S. ; Chun Chen, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks", Computers, IEEE Transactions on (Volume:62 , Issue: 3), March 2013.