New Approach to Implement Authentication and Key Distribution on WI-Max Networks

G. Ramasubbareddy[1]
Research Scholar,
Department of CSE,
Sunrise University,
Alwar (Rajasthan)

Dr. S. Balaji [2]
Professor
Department of CSE,
Sunrise University,
Alwar (Rajasthan)

Abstract: Wi-Max is utilized for the remote system. This innovation will be a developing innovation for remote innovation in future. It is like Wi-Fi however its territory of scope and transfer speed is considerably higher than the Wi-Fi. So the security turns out to be vital issue. Wi-Max innovation incorporates some security components, for example, Key administration, Authentication and privacy. For security first need is crosswise over remote system and other is to give get to control to the system and the get to control can be given utilizing access control conventions. Major issues are in WiMax difficult to handle the security problems. In this paper proposed implementing authentication and distribution of keys in secure manner on open networks and also providing confidentiality.

Keywords: *WI-Max, Authentication, confidentiality, key management, Distribution of keys.*

*****

I. Introduction:

WiMAX is the media transmission innovation, which was made with the intend to supply the high range of contraptions with the comprehensive remote system. The articulation "WiMAX" was made by the affiliation WiMAX Forum, which was set up in 2001 with the intend to encapsulate the innovation of WiMAX in life. Social occasion depicts WiMAX as the innovation in light of the uncommon standard, which outfits the client with the quick access to the remote system. The most hoisted speed is 1 Gbit/s. WiMAX is useful for the course of action of such issues: the relationship of the motivations behind Wi-Fi with each other and distinctive segments of the Internet; the supply with the fast servers of data transmission and media transmission benefits; the development of the remote get to centers which don't depend around upon the geological position; the generation of the checking systems. WiMAX enables to get fast access to the Internet with the more made net than the Wi-Fi systems. The issue of the last mile has reliably been the basic issue for the Internet providers. It is the short name of worldwide interoperability for Microwave gets to. It is the trademark for the gathering of media transmission arrange. Wi-Max is depicted in IEEE 802.16 remote metropolitan zone arrange (MAN). It is the broadband remote innovation It is the short name of Worldwide interoperability for Microwave get to. It is the trademark for the gathering of media transmission organizes. Wi-Max is depicted in IEEE 802.16 remote metropolitan domain organize (MAN). It is the broadband remote innovation.

Wi-max base station: It contains indoor gadgets and a Wi-Max tower. Wi-Max Subscriber Station: It is the beneficiary which gets to the organization of base station Range: 30 mile (50 km) Speed: up to 75Mbps Recurrence band: 2 to 11 GHz and 10 to 66 GHz (approved and unlicensed groups).Its scope territory is approx 50km (30 mile), Bit rate is 75 Mbps, Wi-Max bolster both direct to Point and point toward multi point topology.

II. Existing Systems::

2.1 Privacy:

In existing method there no privacy for data and proper procedure for key management. Using symmetric encryption algorithms for privacy of the data. Like DES and Triple DES. But symmetric cryptography algorithms not provide such must of privacy. The 128-bit or 256-bit key used for deriving the cipher is generated during the authentication phase and is periodically refreshed for additional protection.

2.2 Authentication:

WiMAX provides a flexible means for authenticating subscriber stations and users to prevent unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards.

 ISSN: 2321-8169
819 – 821

2.3 Flexible Key-management Protocol

The Privacy and Key Management Protocol Version 2 (PKMv2) is used for securely transferring keying material from the base station to the mobile station, periodically re-authorizing and refreshing the keys.

1.4 Support for Fast Handover

To support fast handovers, WiMAX allows the MS to use pre-authentication with a particular target BS to facilitate accelerated re-entry.

A three-way handshake scheme is supported to optimize the re-authentication mechanisms for supporting fast handovers, while simultaneously preventing any man-in-the-middle attacks.

III. Proposed Systems:

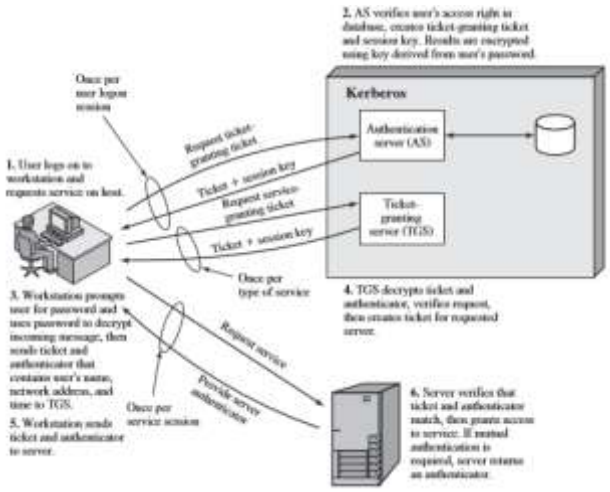
In paper we proposed efficient authentication and key distribution methods used to overcome the existed problems. For authentication using Kerberos algorithms similarly various methods are using for key management and distribution.

3.1 Authentication:

Kerberos4 is an authentication service. Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. an unauthorized user may be able to gain access to services and data that he or she is not authorized to access. Rather than building in elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

1. The client requests a ticket-granting ticket on behalf of the user by sending its user's ID to the AS, together with the TGS ID, indicating a request to use the TGS service.

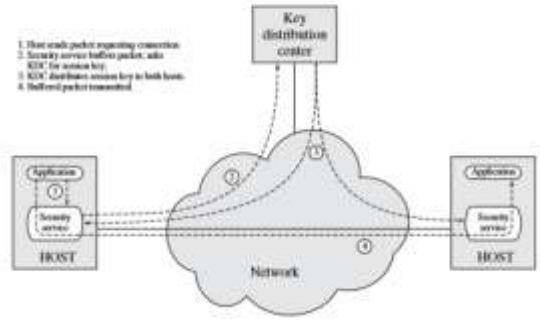
2. The AS responds with a ticket that is encrypted with a key that is derived from the user's password (Kc), which is already stored at the AS. When this response arrives at the client, the client prompts the user for his or her password, generates the key, and attempts to decrypt the incoming message. If the correct password is supplied, the ticket is successfully recovered.



3.2 Key distribution:

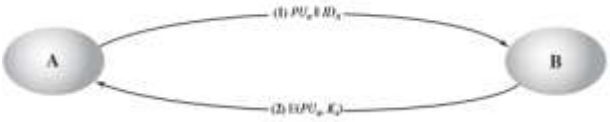
Key distribution is the function that delivers a key to two parties who wish to exchange secure encrypted data. Some sort of mechanism or protocol is needed to provide for the secure distribution of keys.

Key distribution often involves the use of master keys, which are infrequently used and are long lasting, and session keys, which are generated and distributed for temporary use between two parties.



3.3 Symmetric key distribution using Asymmetric Encryption:

1. A generate key pair for transmits a message to B, it consists of public key of A and identity of user A.
2. B generate secret key and transmit to A with encrypt using user A public key.
3. User A decrypt the message using A private key use secret key transmits the data.

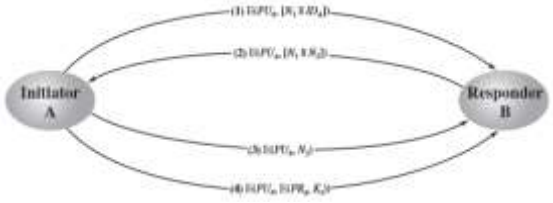


3.4 Secret Key Distribution with Confidentiality and Authentication

This approach provides the protection from both passive and active attacks. Similar to previous approach but some special transactions are providing reliability service.

 ISSN: 2321-8169
819 – 821

Share the identities with their respective key pairs and also share the session's keys to make more secure. And also some challenge questions are transmit the each other for authenticate.



IV. Conclusion:

Security is a major issue in wireless environment, need to protect for every transaction. In existing using symmetric algorithms for authentication and key distribution but this approach not sufficient for wireless network and easy to effect by attacks. In this paper we proposed asymmetric key distribution for exchange the keys with secret keys. For authentication use Kerberos algorithm.

References:

[1] V. Gunasekaran, F. Harmantzis, "Emerging wireless technologies for developing countries", Technology in Society 29 23–42, 2009.

[2] V. Abel, "Survey of Current and Future Trends in Security in Wireless Networks", International Journal of Scientific & Engineering Research (ISSN 2229-5518), April 2011

[3] V. Abel, A. Mnaouer, "On the Study of the WiMAX Security Threats and Current Solution Trends", Journal of the Caribbean Academy of Sciences, 2010.

[4] N.Sastry, J. Crowcroft, K. Sollins, "Architecting Citywide Ubiquitous Wi-Fi Access"

[5] R.Barton,S.Hwu,M.Khayat,A.Schlesinger, "Lunar Surface EVA 802.16 Radio Study", NASA – Johnson Space Center, October 13, 2008

[6] V.Abel, R.Rambally, "An Analysis of WiMax Security Vulnerabilities", International conference on wireless networks and embedded systems WECON 2009

[7] V.Abel, "Survey of Attacks on Mobile Adhoc Wireless Networks", International Journal on Computer Science and Engineering, ISSN : 0975-3397, Vol. 3 No. 2, 2 Feb 2011.