KERBEROS IMPLEMENTATION IN MANETS

Atta-ur-Rahman, Mureed Hussain
SZAB Institute of Science and Technology, Islamabad, Pakistan

Kahina Kabri, Dominique Seret
Department of Mathematics et Informatics, University of Paris 5, France

Keywords: Kerberos, MANETs, Authentication, Ah-hoc networks.

Abstract: In this paper implementation of Kerberos is proposed for Mobile Ad-hoc Networks (MANETS) for user authentication and authorization. Kerberos uses symmetric cryptography with a trusted server to enable secure authentication and key exchange between client nodes. Kerberos protocol is designed to provide reliable authentication over open and insecure networks where communications between the hosts belonging to it may be intercepted. So simply Kerberos is an authentication protocol for trusted hosts on un-trusted networks. There are two approaches used in MANETS: proactive approach & reactive approach. In proactive approach protocols are also known as traditional distributed shortest-path protocols which are used to maintain the routes at all times based on periodic updates with high routing overhead. We have implemented Kerberos concept with proactive approach using Optimized Link State Routing Protocol (OLSR).

1 INTRODUCTION

There are two basic wireless network topologies such as infrastructure based networks and infrastructure less networks also known as ad-hoc networks. The combination of both networks is called Heterogeneous Wireless Network or Heterogeneous Mobile Ad-hoc Networks. Mobile nodes move in cells in mobile and ad-hoc networks. Structure of mobile ad-hoc networks is same as general mobile networks, but difference lies in their ability to self-configuring network of mobile nodes. Ad-hoc networks do not need any backbone infrastructure support and are easy to deploy. MANETS are useful when infrastructure is absent, destroyed or impractical. Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs which communicate over radio and do not need any pre installed communication infrastructure. Communication can be performed if two nodes are close enough to exchange packets.(Security in Adhoc Networks)

In context of security in MANETs, apart from traditional to these classical threats, there are various special threats in MANETS, e.g. denial of service attacks against the energy resource can be performed by using any of the services a node is offering.(Karygiannis, 2002). In MANETS security and user authentication are still an unresolved and challenging research area. In case of disaster areas it is especially important to restrain unauthorized nodes accessing the networks by implementation of an authorization scheme (Security in Adhoc Networks).

2 REQUIREMENTS AND ARCHITECTURE

To fulfil the authentication mechanisms of MANETs there are various considerations which need to be taken into account:

1. The MANETs topology is table driven and dynamic.
2. MANETs may be globally connected with other networks.
3. The MANETs has an addressing scheme with Duplicate Addressing Detection (DAD) mechanisms.

ur-Rahman A., Hussain M., Kabri K. and Seret D. (2008).
KERBEROS IMPLEMENTATION IN MANETS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 161-166
DOI: 10.5220/0001930401610166

4. In OLSR MPR may also function as KDC server.
5. The mobile nodes support security protocols like IPSec.
6. Access to network resources is restricted to only for authorized nodes.
7. The mobile nodes are preconfigured with security credentials to perform their authentication procedures.

For a best viewing experience the used font should be Times New Roman, on a Macintosh use the font named times, except on special occasions, such as program code (Section 2.3.7).

3 OLSR IN ADHOC NETWORKS

OLSR is a proactive routing protocol for MANETS. This protocol inherits the stability of link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol, tailored for mobile ad hoc networks.

The OLSR is a table driven and proactive protocol, as it is used to exchange topology information with other nodes of the network regularly and proactively. The nodes which are selected as an intermediate nodes call multipoint relay (MPR) (2-Level Authentication Mechanisms, 2006).

Neighbour nodes announce this information periodically in their control messages. The protocol uses the MPR to facilitate efficient flooding of control messages in the network. The advantage of this approach is that connections are established quickly. M*ultipoint relays* reduce the size of the control messages. This technique significantly reduces the number of retransmissions of broadcast control messages. OLSR is characterized by two types of control messages: neighborhood messages and topology messages, called respectively *Hello* messages and *Topology Control* (*TC*) messages. MPRs have been shown below in solid black circles:

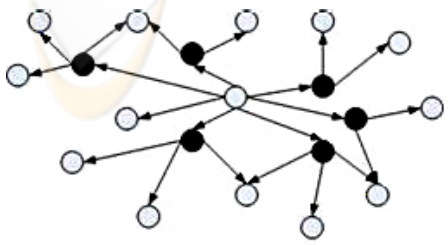

Figure 1: Multipoint Relays Selection (MPRs).

3.1 Neighbour Discovery

Each node must detect its neighbour nodes with which it has a direct link. Due to the uncertainties in radio propagation, a link between neighbouring nodes may enable the transmission of data in either one or both directions over the link. For this, each node periodically broadcasts *Hello* messages, containing the list of neighbours known to the node and their link status, as shown in Fig 3.

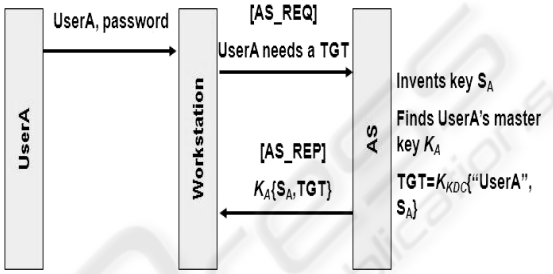

Figure 2: Obtaining TGT.

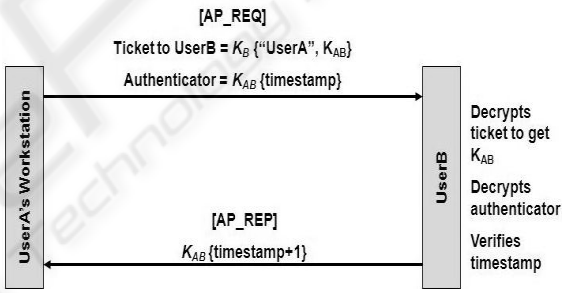

Figure 3: Ticket Granting Mechanisms.

The MPR set is chosen so that a minimum of one-hop symmetric neighbors are able to reach all the symmetric two-hop neighbors. In order to calculate the MPR set, the node must have link state information about all one-hop and two-hop neighbors. This information is, as already mentioned, gathered from HELLO messages

Thus, *Hello* messages enable each node to discover its one-hop neighbors, as well as its two-hop neighbors (the neighbors of its neighbors). Each node of the network independently selects its multipoint relays (Karygiannis, 2002)

Each node keeps a table of routes to all known destinations, through its MPR nodes. Every node periodically broadcasts list of its MPR Selectors (instead of the whole list of neighbors). Upon receipt of MPR information each node recalculates and updates routes to each known destination.

4 RELATED WORK

In context of secure protocols for sensor networks, Wireless Encryption Protocol (WEP) is playing a vital role to secure link-level data during wireless transmission between clients and intermediate devices. WEP protocol is not designed for end to end data. It only works from node to intermediate device (Karygiannis, 2002).

There are two types of authentication systems; open system authentication and shared key authentication system based on cryptography. The open system intermediate devices accept the nodes without verifying the identity. So there is an only one way authentication mechanism in which only intermediate devices are authenticated by the nodes (Karygiannis, 2002). In shared key scenario a node is allowed to join network with WEP shared key.

So the open system is highly vulnerable to attacks and openly invites unauthorized users and nodes. But in case of shared key authentication which is also known as cryptographic approach based on the fact that client has knowledge about the shared secret.

802.11 standard supports privacy through the use of cryptographic techniques for the wireless networks. The WEP (Karygiannis, 2002) also uses the RC4 symmetric key stream cipher algorithms to generate the pseudo-random data sequences, and this key stream simply adds modulo 2 to the data to be transmitted. WEP protocol is applicable all over the 802.11 layers to protect the traffic such as TCP/IP, IPX and HTTP (Karygiannis, 2002).

There are various problems in WEP protocol reported by various group of computer security specialists. These includes the passive attacks based on the statistical data analysis for which integrity can be compromised because of static WEP Key which is shared for long time of period with plain text frame transmission in WEP (Karygiannis, 2002). There is no user authentication in the WEP protocols mean only Service Set Identifier (SSID) identification occurs and nodes authentication is simple and based on shared key.

Another authentication technique proposed by Zhangyan (Security in Adhoc Networks) with the help of implementation of external Certificate Authority (CA) and tamper-resistant chip to support ubiquitous security in the MANETS. This technique uses broadcast blacklist and shared password to normal nodes using broadcast encryption.

The external CA used for this purpose which can issue public key pair and its certificates to every node and publish public key, so there is trust model based on CA between nodes. In case some nodes are compromised, the external CA joins network to broadcast the blacklist (compromised node list) and new password to the legitimate devices. Another key is issued by the CA through broadcast called encryption root key and child key issued to the legitimated nodes broadcast encryption root key is used for encryption and child key is used for decryption.

Another technique which is being employed in (Security in Adhoc Networks) is tamper resistant adhoc chip which can be embedded into any adhoc node or device to support the external CA based security solutions.

In this technique there is a problem that existing nodes cannot be used for adhoc network services because they have not any chip which will recognize by external CA. So this approach is not appropriate for existing devices and there should be special nodes with tamper resistance adhoc chips.

Another approach is proposed by Andreas Hafslund and Jon (2-Level Authentication Mechanisms, 2006). In this approach a 2-level authentication mechanism in an internet connected MANET was proposed. In this approach they proposed in level-1 authentication all the nodes will be authenticated to access the local MANET service or MANET network resources and in level-2 authentication nodes will be authenticated by the external gateway to access the global internet. So in this approach there are two levels of authentication and there is big overhead. Therefore there are chances of DOS and DDOS attacks on gateway nodes or other attacks like IP spoofing. It will also create some problems related to QOS.

5 PROPOSED WORK

The proposed technical measures involve the use of trust model for secure and authorized user access over the networks. The proposed system is based on Kerberos protocol for MANETS. Kerberos is widely used in windows system and is very helpful for user authentication for windows operating system. In an open network environment, a workstation cannot be trusted to identify its users correctly to network services. Kerberos provides an alternative approach whereby a trusted third-party authentication service is used to verify users' identities.

Kerberos is based on secret key distribution model developed by Needham & Schroeder at Massachusetts Institute of Technology (MIT) based on symmetric cryptography. It is based on trusted

server model for secure authentication and Key Exchange between the clients (Zhang).

It is possible to run Kerberos authentication software on more than one machine. However, there is always only one master copy of the Kerberos database. The machine where database is hosted is called master machine or just the master while other machines may possess read-only copies of the Kerberos database, and are called slaves.

In t In this approach basic idea is long lived memorized passwords with short lived session keys (dominate the WEP static key) (Karygiannis, 2002). So it must be kept highly secure.

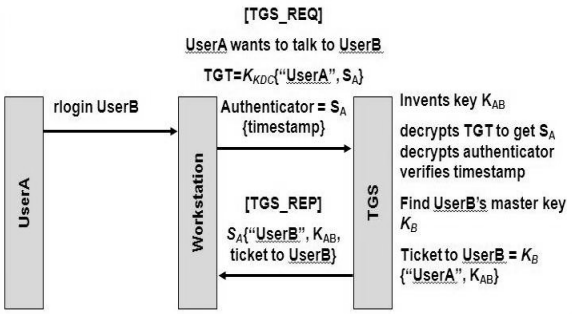

Figure 4: Logging operations.

6 BASICS OF KERBEROS

Kerberos keeps a database of its clients and their private keys. The private key is a large number known only to Kerberos and the client it belongs to. In case that the client is a user, it is an encrypted password. Network services requiring authentication, register with Kerberos, as do clients wishing to use those services. The private keys are negotiated at registration.

Since Kerberos knows these private keys, it can create messages which convince one client that the other is really who it claims to be. Kerberos also generates temporary private keys, called session keys, which are given to two clients and no one else. A session key can be used to encrypt messages between two parties.

A→KDC: *IDA* || *IDB* || *N1*
KDC→A:EKa[Ks||*IDB*||*N1*||E*Kb*[*Ks*||*IDA*]]
(1)
A→B: *EKb*[*Ks*||*IDA*]
B→A: *EKs*[*N2*]
A→B: *EKs*[f(*N2*)]

In the above scenario secure distribution of a new session key for communications between A & B is being taking place.

It becomes vulnerable to replay attack if an old session key has been compromised "A→B: *EKb*[*Ks*||*IDA*]" can be resent convincing B that it is communicating with A. B→A: *EKs*[*N2*] & A→B: *EKs*[f(*N2*)] is used for modification to addresses (time stamps and using an extra nonce)

In ordered to avoid the requirements of synchronization (Woo and Lam, 1992) proposed a structure defined as under.

1. A → KDC: $ID_A||ID_B$
2. KDC → A: $E_{KR_{auth}}[ID_B||KU_b]$
3. A → B: $E_{KU_b}[N_a||ID_A]$
4. B → KDC: $ID_B||ID_A||E_{KU_{auth}}[N_a]$
5. KDC → B: $E_{KR_{auth}}[ID_A||KU_a]||E_{KU_b}[E_{KR_{auth}}[N_a||K_s||ID_B]]$
6. B → A: $E_{KU_a}[E_{KR_{auth}}[N_a||K_s||ID_B]||N_b]$
7. A → B: $E_{K_s}[N_b]$

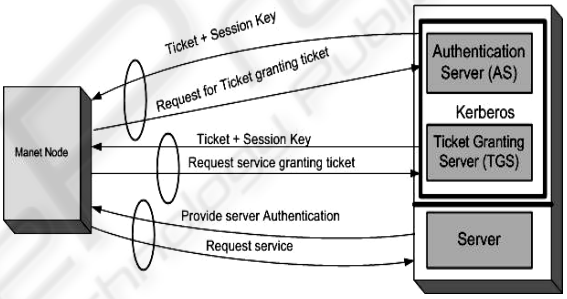

Figure 5: KDC Implementation.

To avoid impersonation, severs must be able to confirm identities, so there should be authentication approach for user authentication so Authentication Server (AS) is used to store the passwords of all users. Authentication Server shares unique secret keys with each server.

Another approach which is used is known as Ticket Granting Service. Kerberos Server shares a secret key with each user which is knows as master key. Kerberos server invents a session key KAB which encrypts master keys of both communicating parties, known as ticket. Therefore master keys derived from the user's passwords and session keys will be used for single session. And the ticket granting ticket is sent to KDC to acquire the session key for communication between two parties, as shown in figure 5.

7 KERBEROS IN MANETS

In MANET MPR or master node will act as Kerberos node that is authentication server (AS) and

will share unique key with each server and Ticket Granting Server (TGS) as well, which will share a secrete key with each user known as Master Key (MK).

MPR or master node which is now working as kerberos server invents a session key K_{AB} when a user A informs to MPR it wants to talk B, then K_{AB} is encrypted with A's Master Key(MK) & with B's Master Key (MK) as well known as ticket. User B can decrypt the K_{AB} and user A's name. Master Key (MK) is derived from user's password. Session Key SA is used by user A for a single session, which will be valid for a small time. Node on behalf of user A asks the Authentication Server (AS) for a session key SA. SA is transmitted & encrypted with user A's MK (Master Key). The MPR (AS) also sends TGT, encrypted with Kerberos Server Master Key (MK). SA use A's name and TGT expiration time. TGT is sent to KDC to acquire the session key for communication between two parties. TGT Server and AS are collocated, means both need to use the same information. Generally Kerberos uses the DES algorithms. Users passwords converts into DES Key & decrypts the information. Once getting the key, Master key (MK) is discarded and only retains the TGT & Session Key (S). The scenario is discussed as under. All ticket generating mechanisms are show in figures 2, 3 and 4.

TGS decrypts the TGT and checks the expiration time then generates KAB with name of user A and expiration time and encrypts with user B's master key KB and all this will be encrypted with SA. Ticket grating scenario is defined as under.

User B keeps track of the recent time stamps. The following scenario shows the login operation of user B.

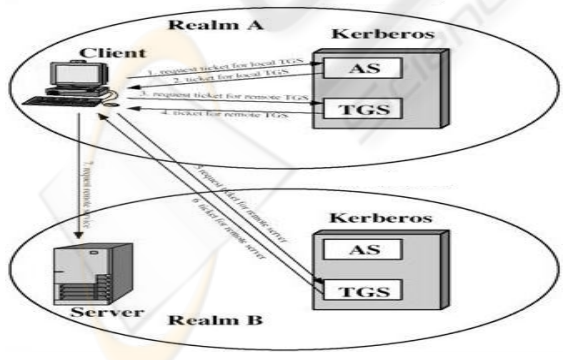

Figure 6: Realms replication.

7.1 Secure Authentication

TGS issues tickets to users who have been authenticated to AS thus only the correct user with the password can acquire ticket. Replication is necessary to avoid a single point of failure in case of single Kerberos Server so there is need of multiple Kerberos Servers. Those will share same Master Key and identical databases. Kerberos Server maintains the master copy, and all other sites will be updated periodically.

7.2 Concepts of Realms in MANETS

Each Kerberos realm has a master Kerberos machine, which houses the master copy of the authentication database. It is possible (although not necessary) to have additional, read-only copies of the database on slave machines elsewhere in the network. The advantages of having multiple copies of the database are those usually cited for replication: higher availability and better performance. If the master machine is down, authentication can still be achieved on one of the slave machines. The ability to perform authentication on any one of several machines reduces the probability of a bottleneck at the master machine (CISCO).

Keeping multiple copies of the database introduces the problem of data consistency. We have found that very simple methods suffice for dealing with inconsistency. The master database is dumped every hour. The database is sent, in its entirety, to the slave machines, which then update their own databases. A program on the master host, called kprop, sends the update to a peer program, called kpropd, running on each of the slave machines. First kprop sends a checksum of the new database it is about to send. The checksum is encrypted in the Kerberos master database key, which both the master and slave Kerberos machines possess. The data is then transferred over the network to the kpropd on the slave machine, s shown in figure 6. The slave propagation server calculates a checksum of the data it has received, and if it matches the checksum sent by the master, the new information is used to update the slave's database (CISCO). All passwords in the Kerberos database are encrypted in the master database key Therefore, the information passed from master to slave over the network is not useful to an eavesdropper. However, it is essential that only information from the master host be accepted by the slaves, and that tampering of data be detected, thus th checksum (CISCO).

Kerberos introduced RC4-HMAC support, which is also present in Windows and is more secure than DES. Among the supported encryptions (but not by Windows) the triple DES (3DES) and newer

AES128 and AES256 are worth mentioning. The Kerberos protocol is to prevent the user's password from being stored in its unencrypted form, even in the authentication server database. Considering that each encryption algorithm uses its own key length, it is clear that, if the user is not to be forced to use a different password of a fixed size for each encryption method supported, the encryption keys cannot be the passwords. For these reasons the string2key function has been introduced, which transforms an unencrypted password into an encryption key suitable for the type of encryption to be used. This function is called each time a user changes password or enters it for authentication. The string2key is called a hash function, meaning that it is irreversible: given that an encryption key cannot determine the password which generated it. Famous hashing algorithms are MD5 and CRC32 is used.

8 CONCLUSIONS

We have proposed a trust model to solve the user authentication problems in the MANET. This mechanism is designed to provide reliable authentication over open and insecure networks where communications between the hosts belonging to it may be intercepted in the MANET. Our idea has the advantages of high security, flexibility and practicality. It can be treated as base-bone to implement secure authentication in the ad hoc networks.

REFERENCES

Tom Karygiannis, Les Owens "CSD, NISTE Gaithersburg", MD 2098, 8930 (2002).

Security in Adhoc Networks by Zhang Yan, networking laboratory Helsinki University of Technology.

2-Level Authentication Mechanisms in an Internet Connected MANET 6th Scandinarian Workshop on Wireless Adhoc Networks (2006).

Yanchoa Zhang, New Jersey Institute of Technology. www.indengines.com Sunnyvale, California 94089 USA. J. Broch, D. Johnson,

Jennifer G. Steiner, Project Athena, Massachusetts Institute of Technology, Cambridge, MA 02139

www.cisco.com/warp/public/106/1.html#intro

Z. J. Haas, M. R. Pearlman, P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," draft-ietf-manetzone-zrp-02.txt, IETF, (2000).

P. Jacquet, P. Muhletaler, A. Qayyum, A. Laouiti, T. Clausen, L. Viennot, "*Optimized Link Stat e Routing Protocol*", in IEEE INMIC, Pakistan (2001).

A. Qayyum, L. Viennot, A. Laouiti, "*Multipoint Relaying: An Efficient Technique for flooding in Mobile Wireless Networks*" Tech. Rep. 3898, INRIA, http:// www.inria.fr, (2000).

Maltz, "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks*", draft-ietfmanet-dsr-01.txt, IETF 1998.

J. Broch, D. A. Maltz, D. B. Johnson, "*Supporting Hieararchy and Heterogeneous Interfaces in Multi-hop Wireless Ad Hoc Networks*", Workshop on Mobile Computing, IEEE International Symposium on Parallel Architectures, algorithms and Networks, Australia pp. 75–85, (1999).

Mounir Benzaid, Pascale Minet, Khaldoun AlAgha, Cedric Adjih and Geraud Allard Integration of Mobile-IP with OLSR for Universal Mobility.

T. Y. C. Woo and S. S. Lam. *Authentication for distributed Systems Computer*, 25(1):39–52, January 1992.