Modification in Kerberos Assisted Authentication in Mobile Ad-Hoc Networks to Prevent Ticket Replay Attacks

Kashif Bashir and Mohammad Khalid Khan

***Abstract*—Security is an important issue for any type of networks, especially for wireless ad-hoc networks. Kerberos tickets used in KAMAN authentication scheme can be captured over the network are prone to replay attacks. The research work described in this document demonstrates that the modification in KAMAN protocol can increase authorization. We are proposed that all of contents are encapsulated in an encrypted packet. So the replay attacks become impossible. Moreover, in the proposed scheme there is no burden on the server and the client to undertake the modified KAMAN process. We also simulate describe architecture and verified that propose methods can reduce the chances of reply attack in MANET using KAMAN as authentication protocol.**

***Index Terms*—KAMAN, reply attacks, security in MANET, confidentiality, non-repudiation.**

I. Introduction

In this section, ad-hoc networks and its security is briefly discussed. An ad hoc network is a set of wireless mobile nodes that form a dynamic autonomous network without the intervention of centralized access points or base stations. There is a need for efficient routing protocols to allow the nodes to communicate over multi-hop paths consisting of possibly several links in a way that does not use any more of the network "resources" than necessary. There are two major types of Ad-Hoc networking.

1) Mobile Ad Hoc Networks
2) Wireless Ad-Hoc Sensor Networks

A Mobile Ad-hoc Network (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e. routing functionality will be incorporated into mobile nodes.

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. The ability of the sensor network to aggregate the data collected can greatly reduce the number of messages that need to be transmitted across the network.

Security in ad-hoc networks is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we have to consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation [1].

II. Authentication in MANETs

Authentication in ad-hoc wireless network requires secure communication. [8] State that ad-hoc network can be secure by having public-key-based key exchange protocol and hash-based alternatives. Authentication in ad-hoc networks is one of the major security issues affecting the wired and the wireless network community. It is generally accomplished in two ways: direct and indirect authentication [3]. In direct authentication, two parties use pre-shared symmetric or asymmetric keys for verifying each other and the flow of data between them. In indirect authentication, a trusted third party, i.e. a Certification Authority, is made responsible for certifying one party to another party. Most of the secure routing protocols developed for ad-hoc networks, rely on indirect authentication mechanisms using public key infrastructures (PKI) to authenticate communicating nodes [5].

The ad-hoc network without any preventive protection for the routing protocol disrupts the network. The proposed solution in [9] is MANET Authentication Extension (MAE) securing Optimized Link State Routing protocol (OLSR) to be appended to each routing protocol message or packet, providing the authentication services. In [10] the proposed protocol, it is described that when a mobile host is moved to the visited domain to enquire any service, it first authenticates itself with the KDC of the public key based Kerberos present in that domain. However public key based Kerberos requires significant computational resources and not all mobile computing domains support public key based Kerberos authentication so interpretability is not always possible.

In contrast, Kerberos [6] is a symmetric key based indirect authentication mechanism. The security and effectiveness of Kerberos has been proven over a long period of time. Kerberos authentication system is now a fairly mature, secure and reliable standard. Kerberos has always been an active area of exploration, examination and application by the research community. Researchers have used Kerberos in order to provide security features in their research project. Various extensions and alternations in the standard in the

Manuscript received April 5, 2012; revised May 2, 2012.

Authors are with the College of Computer and Information Sciences PAF-Karachi Institute of Economics and Technology Karachi, Pakistan (e-mail: kashif@pafkiet.edu.pk, khalid.khan@pafkiet.edu.pk).

standard Kerberos protocol have also been proposed by the researchers.

Kerberos [7] clients authenticate themselves to servers by presenting tickets for each service. Tickets are distributed by a central trusted server within each administrative domain, and are constructed so that only clients possessing the appropriate key(s) are able to decrypt and use them. Kerberos includes specific features to prevent forgery of client or server identity, detect replay attacks, establish secure channels between endpoints through safe distribution of temporary session keys, and minimize the likelihood that the user's Kerberos password will be compromised (it never leaves the user's workstation, and all traces of it are destroyed once the user has authenticated herself). The strengths and weaknesses of Kerberos are analyzed in detail in [4].

In Kaman [2], Kerberos assisted Authentication in Mobile Ad-hoc Networks, a new pure managed authentication service for mobile ad-hoc networks. Kaman is based on the time-tested and widely deployed Kerberos protocol, and provides secure extensions to support the more challenging demands of ad-hoc networks. Kaman migrate a number of features from the traditional, wired Kerberos environments to the ad-hoc environment. Kaman has been specifically designed for hostile environments, in which the presence of malicious nodes and the likelihood of physical node capture are relatively high.

Kaman is a secure authentication scheme, for ad-hoc networks. In Kaman there are multiple Kerberos servers for distributed authentication and load distribution. As mobile nodes are susceptible to physical possession, in Kaman only the users know the secret key or password and the servers know a cryptographic hash of these passwords. All Kaman servers share a secret key with each other server. In Kaman all servers periodically, or on-demand, replicate their databases with each other. Whenever unicast or multicast communication is required among nodes, the nodes approach the Kaman servers whom in turn allocate a session key for their secure authentic communication.

III. Problem in Kaman Protocol

Kerberos tickets used in KAMAN authentication scheme between communication parties is prone to ticket replayed attacks. Figure 1 shows, two different problems occur in KAMAN Authentication Scheme during the communication between two nodes.

1) In KAMAN the mobile node C1 connects to the Kerberos servers S1 whenever it desires to undertake a secure communication with C2.As response S1 sends an encrypted ticket and an encrypted session key to client C1.The session key is a random key generated by server S1. The problem is that here this ticket can be captured by the hostile user on the network and can be replayed by the hostile user at any later time in order to access the service.
2) In KAMAN after getting ticket from S1 ,client C1 sends this ticket to client C2.At this stage this ticket can be captured.

IV. Proposed Solution

It is obvious from the previous section that are some proposing modification in communication messages are required in the original KAMAN protocol in order to provide a secure communication in ad-hoc networks. These changes are required during the two phases, rest of the communication between client and application service remains same as in case of original KAMAN.

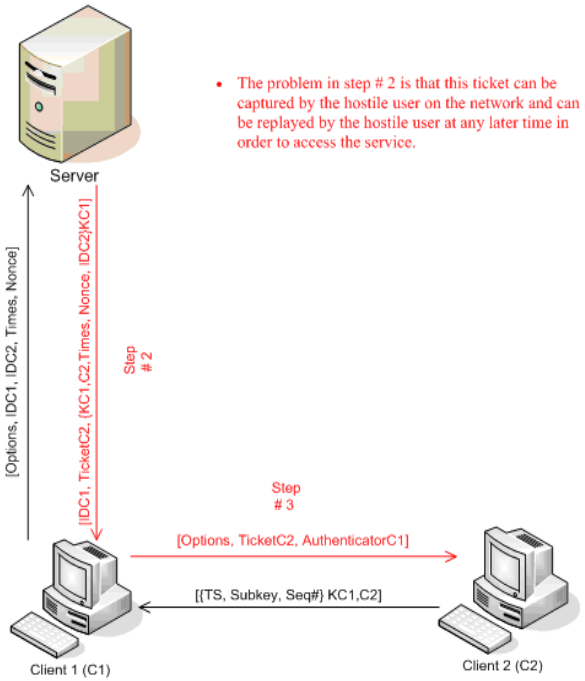


Fig. 1. Two different problems occur in KAMAN authentication scheme during the communication between two nodes.

This selection provides the general idea about the overall working of the scheme.

In KAMAN the mobile node C1 connect to Kerberos server S1 whenever it desires to undertake a secure communication with C2.As response S1 sends an encrypted ticket and an encrypted session key to client C1.Problem is that here this ticket can be captured by the hostile user on the network and can be captured by the hostile user at any later time in order to access the service.

Now the idea, which is proposed, is that s1 should generate a session key and a ticket. Server S1 now sends all above two things back to C1, in a packet. This packet is encrypted with the key derived by the password of C1. Now C1 decrypts packet it gets from S1 and find 2 things, without capturing.

In KAMAN, after getting ticket from S1, C1 now sends this ticket to C2. But as in the 1st step, this ticket can be captured here too.

In my proposed idea (Figure 2), when C1 gets two things from S1; i.e. ticket, session key and a key derived. Then C1 sends the ticket and its authenticator in a packet form to C2. This packet is encrypted with the key derived from the password of C2 and will sent by S1 to C1. So the danger of ticket capturing is eliminating.

The high level overview or overall working of the modified KAMAN has already been described in above. This section discusses the inner details of the modified KAMAN protocol.

Some notations were used in KAMAN [1] to describe the original KAMAN protocol. Those notations are also used here to describe the modified KAMAN protocol. The notations are

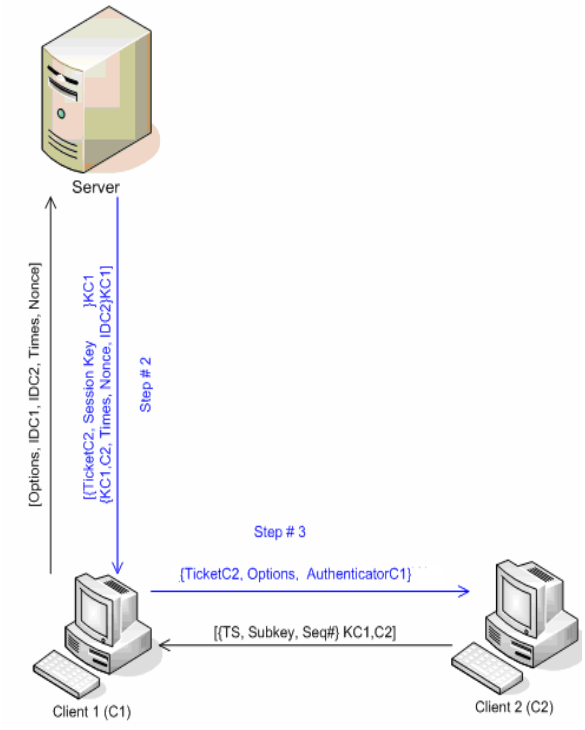


Fig. 2. Modified KAMAN authentication scheme

Options: used to request that certain flags be set in the returned ticket.

Times: used to specify the start, end and renewal time settings in the ticket.

Flags: status of the ticket.

Subkey: choice for another encryption key for this session instead of Kc1, c2

IDc1 : identity of client1

IDc2 : identity of client2

ADc1: network address of client1

Kc1, c2: session key between client1 and client2

TS : informs of time when this authenticator was generated.

Apart from this the above notations, the modified KAMAN protocol also introduce its own notations.

Kc1 : encryption key based on hashed password of client1

Session key: made by applying hash on a shared key between servers

Whenever a node wants to establish a secure connection with another node it approaches the Kerberos server and follows.

Client1 → Server

Option, IDC1, IDC2, Times, Nonce

Server → Client 1

{Ticket, KC1C2, KC2, Times, Nonce, IDC1, IDC2} KC1

Client1 → Client2

{Option, Ticket, AuthenticatorC1}

Client2 → Client1

{TS, Subkey, Seg #}KC1C2

Ticket = {Flags, KC1C2, IDC1, ADC1, Times} KC2

AuthenticatorC1= {IDC1, TS} KC1, C2

V. Implementation

This section discusses the practical usage and implementation of the modified KAMAN protocol. For this purpose a simulation has been designed and coded which makes use of the modified KAMAN protocol to perform authentication and authorization operations. The simulation consists of a server side application, multiple clients may connect to this service and query this service to retrieve the system information of the server on which this service is running. Service requires clients to be authenticated before serving their requests. Similarly, a client may also wish to authenticate the service prior to sending any request. However service only sends that session key, which the client is authorized to access. All the authentication and authorization operations take place using the modified KAMAN protocol which has already been discussed in complete detail in the previous section.

A. Original KAMAN

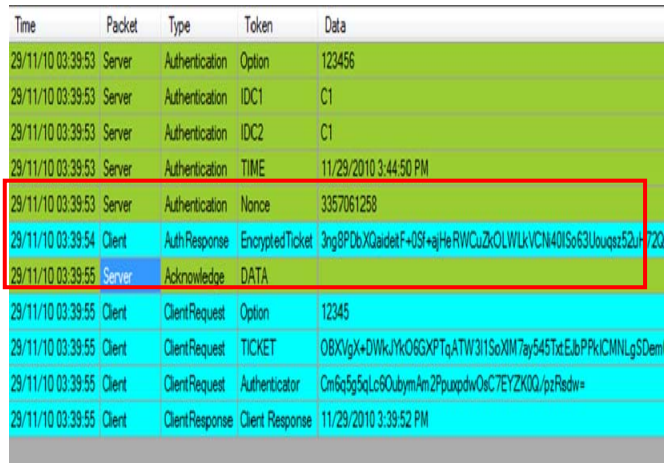
Fig. 3 shows original KAMAN Authentication Scheme simulation. This simulation depicts that how the original KAMAN transmits the packets. Figures show that three things client id, ticket and session key are sent from server to client-1. The security issue that we have identified is shown in this image that the data sent from the server to the client is not encapsulated in one packet but in individual form, and it can be captured. The data marked by line highlights the packets that can be captured and can be used for replay attacks.

Time	Packet	Type	Token	Data
29/11/10 03:48:33	Server	Authentication	Option	123456
29/11/10 03:48:33	Server	Authentication	IDC1	C1
29/11/10 03:48:33	Server	Authentication	IDC2	C1
29/11/10 03:48:33	Server	Authentication	TIME	11/29/2010 3:53:32 PM
29/11/10 03:48:33	Server	Authentication	Nonce	3564226551
29/11/10 03:48:34	Client	AuthResponse	EncryptedTicket	C1
29/11/10 03:48:34	Server	Acknowledge	DATA	
29/11/10 03:48:34	Client	ClientRequest	Option	12345
29/11/10 03:48:34	Client	ClientRequest	TICKET	tFDzOUn9M3FMsQzgUqK8Fj92TRqq6BIFnqSLJct7m66
29/11/10 03:48:34	Client	ClientRequest	Authenticator	uF67o2FAfSiqxjGGEaxqfF0Pw1fufnHfXuQEfSkiwVo=
29/11/10 03:48:34	Client	ClientResponse	Client Response	11/29/2010 3:48:33 PM

Fig. 3. Original KAMAN authentication scheme simulation

B. Modified KAMAN

In Fig. 4 shows Modification in KAMAN Authentication Scheme simulation. In this modified version of KAMAN what we have simulated that after the modification the data will be sent in an encrypted single packet, which will solve the identified problem. In this situation intruder cannot find ticket. The marked text in the above image shows that the data is transmitted in encrypted format and in the form of a single packet.



Time	Packet	Type	Token	Data
29/11/10 03:39:53	Server	Authentication	Option	123456
29/11/10 03:39:53	Server	Authentication	IDC1	C1
29/11/10 03:39:53	Server	Authentication	IDC2	C1
29/11/10 03:39:53	Server	Authentication	TIME	11/29/2010 3:44:50 PM
29/11/10 03:39:53	Server	Authentication	Nonce	3357061258
29/11/10 03:39:54	Client	Auth Response	Encrypted Ticket	3ng8PDbXQaidetF+0Sf+ajHeRWCuZkOLWLkVCN40lSo63Uouqsz52uH72Q
29/11/10 03:39:55	Server	Acknowledge	DATA	
29/11/10 03:39:55	Client	Client Request	Option	12345
29/11/10 03:39:55	Client	Client Request	TICKET	OBXVgX+DWkJYkO6GXPTqATW3I1SoXlM7ay545TxtEJbPPkICMNLgSDem
29/11/10 03:39:55	Client	Client Request	Authenticator	Cm5q5g5qLc6OubymAm2PpupdwOsC7EYZK0Q/pzRsdw=
29/11/10 03:39:55	Client	Client Response	Client Response	11/29/2010 3:39:52 PM

Fig. 4. Modification in KAMAN authentication scheme simulation

VI. Future Work and Conclusion:

When we use MANET there are lots of authentication issues, when we discuss in KAMAN authentication scheme, apply on communication parties, so the ticket can be captured by the hostile users. In this document we are proposed that all of contents are encapsulated in an encrypted packet. So the replay attacks become impossible. When we use MKAMAN we will have to increase more processing speed and more hardware requirement for servers and clients. In future work the impact of security mechanism on the network performance in terms of hardware requirement and processing speed can be investigated.

References

[1] L. D. Zhou and Zygmnunt, "Securing ad hoc networks," *Published in IEEE network, special issue on network security*, November/December, 1999

[2] A. A.Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-hoc Networks," *Proceeding of the 27th Australasian Computer Science Conference*, 2004.

[3] A. Fox and S. Gribble, "Security On the Move: Indirect Authentication Using Kerberos."

[4] S. M. Bellovin and M. Merritt, "Limitations of the Kerberos Authentication System," *Proceedings of Usenix Winter Conference*. 1991: pp. 253-267.

[5] A. A. Pirzada and C. McDonald, "A Review of secure Routing Protocols for adhoc Mobile Wireless Networks," (To be published in) *Proc. Of 2nd workshop on the Internet, Telecommunications and Signal Processing* (DSPCS'03 and WITSP'03), 2003.

[6] J. Kohl and S. Neuman, "The Kerberos Network authentication Services (V5)," RFC 1510, 1993.

[7] Y. C. Zhang, W. Liu, W. J. Lou, and Y. G. Fang, " Securing Mobile Ad Hoc Networks with Certificateless Public Keys," *Published by the IEEE Computer Society*, October, 2006

[8] D. Balfanz, D. K. Smetters, P. Stewart, and H. Chi Wong, "Authentication in Ad-Hoc Wireless Networks," *Network and Distributed System Security Symposium*, 2002.

[9] R. S. Puttini, Ludovic Me, and Rafael Timoteo de Sousa, "Certification and authentication services for securing MANET routing protocols," In *Proceedings of the 5th IFIP TC6 International Conference on Mobile and Wireless Communications Networks*, Singapore, October 2003.

[10] B. Zhang and J. X. Wu, "Authentication and Key Distribution Methods in Mobile Computing Environments," *Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing.* October 2003, pp. 353-356.