Black Hole Attack in Kerberos Assisted Authentication Protocol

Navjot Singh
Department of Computer Science Engineering
Lovely Professional University
Jalandhar, Punjab, India

Rupinder Kaur Cheema
Department of Computer Science Engineering
Lovely Professional University
Jalandhar, Punjab, India

ABSTRACT

Kaman is the extension of Kerberos protocol; with the use of Kaman nodes in the ad hoc network are authenticated by the secure server. This posed the remedial venture to large number of attacks like replay attack, fabrication, eavesdropping etc Kaman provides secure solution to the problem of secure channel establishment, secure exchange of session keys and prevention of nodes identity forgery. In this paper, we reviewed the Kaman; Kerberos assisted Authentication in Mobile Ad hoc Network. We have also emphasized the problem of black hole that aroused when Kaman protocol is embedded into large network.AODV, on-demand routing protocol had been used to select secure shortest path, when node interacts with an authenticated server for mutual authentication.

KEYWORDS

Black hole, Mutual Authentication, Secure server, Ad-hoc networks.

1 INTRODUCTION

An ad-hoc network is infrastructure less network in which each node interacts with other nodes directly or in-directly without the presence of any central controller. When two nodes interact with each other directly they must be in the range of each other and when two nodes are not in each other's vicinity, they had to interact with each other in-directly. When two nodes interact indirectly, intermediate nodes between the two collocate with each other and thus facilitate data forwarding. To establish efficient direct or in-direct communication link between the independent nodes of ad-hoc network, a trust relationship must be maintained between every node in ad hoc network. An efficient mechanism to maintain trust relationship between every node in ad hoc networks is mutual authentication. Before communicating, with other nodes in the network, every node must be mutually authenticated. This has prevented many types of active and passive attacks.

Authentication can be accomplished in two ways:-

- Direct authentication.
- Indirect authentication.

In direct authentication, both parties use symmetric and asymmetric authentication algorithms for authentication. Whereas, in-direct authentication incorporated the use of third party. Third party is used as the certification authority and is responsible for issue of public certificates to the valid legitimate party. Many type of denial of services attacks, are possible in direct and indirect authentication schemes. Authentication scheme proposed in the Kerberos authentication is a hybrid type of authentication scheme. Kerberos scheme is the combination of indirect and direct authentication. Kerberos authentication scheme provides many significant features like: prevention from reply attacks, establishment of secure channel, prevention of nodes original identity, mutual authentication.

Related Work is presented in section 2. We have presented detail of Kaman in section 3.In section 4, details of AODV protocol is written and in the section no 5 we have presented the black hole attack, which arises when Kaman is embedded into larger network. In section 6, 7 conclusion and Future work have been explained, followed by the references in section 7.

2 RELATED WORKS

Yixin Jiang, Chuang Lin had proposed a new mutual authentication and key exchange protocol. The two main features of this protocol are identity anonymity and session key renewal. The proposed protocol is based on the secret splitting principle and self-certified scheme. The protocol works in two phases: First phase is the mutual authentication with anonymity which hides the use's real identity when a legitimate user is roaming from the home agent to the visiting agent. This phase uses the temporal identity (TID) instead of the user's real identity. Second phase is the session key renewal phase which renews the shared key which is shared between the legitimate user and the serving agent [1].Muti-server authentication scheme enables the remote user to access the services of multiple servers without authenticating to each server. In the multi-server architecture, two type of servers are there, one is the services server, which is open to all legitimate users and second is the registration server which has been kept secret and works at the backend. The multi-server authentication server provides some additional features like secure communication between user and services that had been maintained by the establishment of a session key and calculation of secure hash function (HMAC), to provide data confidentiality and data integrity [2].The major limitation of the Kerberos authentication scheme are the basic assumptions that we consider while implementing the Kerberos authentication in the real environment that has been stated as that Kerberos authentication system fails if the assumption gets falsified. The shortcomings of Version4 Kerberos authentication scheme had been worked upon by the version 5 but it required upgradation in hardware. Replay attack, password-guessing attack, spoofing login attack, session key

expose attack is the major attacks which can be triggered while relying on Kerberos authentication scheme. The major limitation is the burst of message exchange that is needed for successful authentication and consequently leads to deterioration of battery performance [3].The Ad hoc on demand routing vector (AODV) is secure and shortest path selection algorithm in Mobile ad hoc network. The source node when needs a shortest path to destination node, it firstly broadcasts RREQ message to its adjacent nodes and in response receives RREP message from every node and then shortest path had been selected on the basis of the metrics viz the hop count and sequence number [4].The authors demonstrated the concept that, Kerberos assisted authentication scheme provides the secure solution to the mutual authentication. When a node wants to communicate to the other nodes, it firstly needs to authenticate itself to the secure server, on the successful accomplishment of the same; Server facilitates the data exchange between the two nodes by the intervention of the encrypted shared key [5].

3. KERBEROS ASSISTED AUTHENTICATION SCHEME IN MOBILE AD HOC NETWORKS

Kaman is the hybrid type of authentication scheme which is proposed by A.A Pirzada and C.McDonald.To prevent various types of active and passive attacks in wireless ad-hoc network, every node in the ad-hoc network should be mutually authenticated Kerberos is a symmetric, key based, indirect authentication scheme. Three assumptions are taken into consideration while implementing Kaman these assumptions are:

- Hashed passwords of all users are stored in the server, all users have passwords and they are only known to them.
- All servers are mutually authenticated and share a secret key.
- All servers shared secrete key .Repository are encrypted with the secrete key when replication takes place.

Kerberos assisted authentication scheme is the extension of the traditional Kerberos authentication. In traditional Kerberos authentication scheme three parties are involved while authentication: first party is the node, which is authenticated by the authentication server, second is the ticket grant party who works on the behalf of the node while authenticating and third party is the authentication server. A huge number of message exchanges are needed for successful authentication and this approach is not an efficient approach when mutual authentication is needed in ad hoc type of network. In Kaman only two parties are involved first is the node which is authenticated by the authentication server and other is the authentication server. There has been the requirement of fewer messages for successful authentication. In Kerberos assisted authentication protocol secure servers are distributed throughout the network and secure hashed passwords are stored on the secure server and servers are self replicated. The secure servers are also mutually authenticated. When the secure server will compromise whole network will be compromised this is the single point of failure in the Kerberos assisted authentication protocol. Election mechanism is used to select the secure server. When the secure servers are not available for mutual authentication, election mechanism will be initiated. When mobile nodes are successfully authenticated with secure server, secure session will be established between the mobile node and secure server to encrypt communication. Initially only the single server excites all the hashed passwords of the users are stored. All the trusted users have assigned higher priority then non-trusted users. Trust level of the users is assigned on the basis of the usage. When the secure servers are not available mutual authentication, user with the higher priority becomes the secure servers and replicates itself with the exciting secure servers. In the replication process repository of the secure server will be replicated. The replication process will be shown in the figure 1

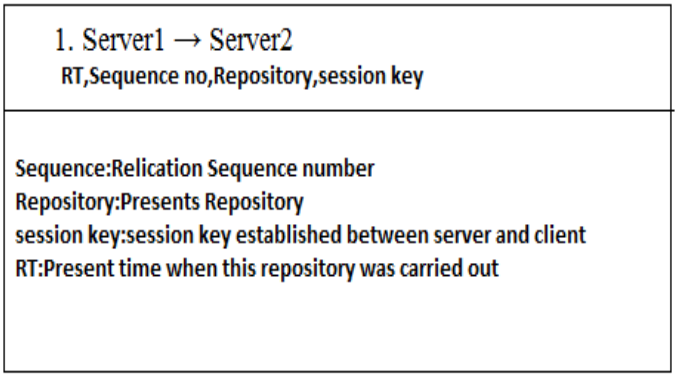

Fig 1: Server Replication Process

3.1 Details of Kaman

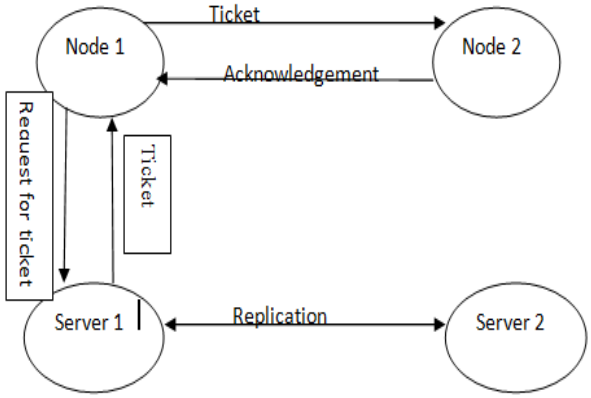

Fig 2: Operations of Kaman

Figure 1 shows the operating mechanism of the KAMAN model. In this, we have got two nodes node1 and node2 along with two servers, server1 and server2.If Node 1 wishes to communicate with Node e 2 .So prior to communication, there must be mutual authentication established between the two parties. For mutual authentication Node 1 requests to its nearest server say Server 1 in this case. When Node 1 gets successfully authenticated to Server 1, Server 1 then issues Ticket to Node 1. Afterwards, Node 1 passes that Ticket to Node 2 .When Node 2 receives, the Ticket it sends acknowledgement to Node 1. Ticket contains the shared key which is generated by Server 1. Data exchanged between Node 1 and Node 2 is encrypted by using shared key. Server 1 and Server 2 both are mutually authenticated. The servers are self replicating and keep on producing their replicas from time to time. In KAMAN, we have assumed that hashed passwords

are stored on the authentication servers and each server is mutually authenticated with other server.

From Node1 to Server
Request For Ticket: Options, IDC1, IDC2, Times, Nonce
From Server to Node1
Ticket: IDN1, Ticket N2, {KN1,N2, Times, Nonce, IDN2}KN1
From Node1 to Node2
Ticket: Options, TicketN2, AuthenticatorN1
From Node2 to Node1
Acknowledgement: {RT, Subkey, Sequence }KN1,N2
TicketN2= {Flags, KN1,N2, IDN1, ADN1, Times}KN2 **AuthenticatorC1=** {IDN1, TS}KN1,N2

Table1: Message exchange in Kerberos assisted authentication Protocol

Following are the various keywords of message exchange in Kerberos assisted authentication Protocol:

- 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
- Nonce: A random value used as a pseudo-unique transaction identifier to avoid replay attacks
- Subkey: Choice for another encryption key for this session instead of KN1,N2
- Sequence: Starting sequence number to detect replays
- IDN1: Identity of Node1
- IDN2: Identity of Node2
- ADN1: Network Address of Node1
- KCn: Encryption key based on hashed password of user n
- KN1, N2: Session key between Node1 and Node2
- RT: Informs of time when this authenticator was generated

4. DETAIL OF AODV

Ad hoc on demand Vector (AODV) is a reactive routing protocol .Reactive means route between source to destination will be established on demand basis. Two important type of control messages are exchanged between the various nodes of Ad hoc networks while establishment of a route. These messages are: RREQ (Route Request) message, RREP (Route Reply) message.

Fig.2 shows the process of route establishment in AODV protocol. Source node S, starts broadcasting RREQ control messages to its reachable nodes with A, B, C as the initial sequences. When reachable node receives RREQ control message it again broadcasts REEQ message to its further reachable nodes. Node A broadcasts RREQ message to its reachable node D which is the destination node. When Node D receives RREQ message, it responds to Node A with RREP message and incremented sequence number. Node A simply forwards same message with same sequence number which it receives from Node D to Node S. When Node S receives RREP message it checks the sequence number and hop count of received RREP message .Now the route is established form Node S to Node A and from Node A to Node D.

5. BLACK HOLE ATTACK IN KERBEROS ASSISTED AUTHENTICATION PROTOCOL

In figure 3 Illustrations, Node 3 starts broadcasting RREQ control message to its reachable node, which furthers forward the broadcasting process. Node 3 receives RREP response from node 4 and node 2. node 4 does not have any direct path to server 1 .But node 3 selects best path to server 1 through node 4 on the basis of hop count and sequence number. When node 3 requests, for ticket to server through node 4 but node 4 is corrupted node and responsible for packet dropping. Thus node 3 has been waiting for the ticket. This attack is called black hole attack.

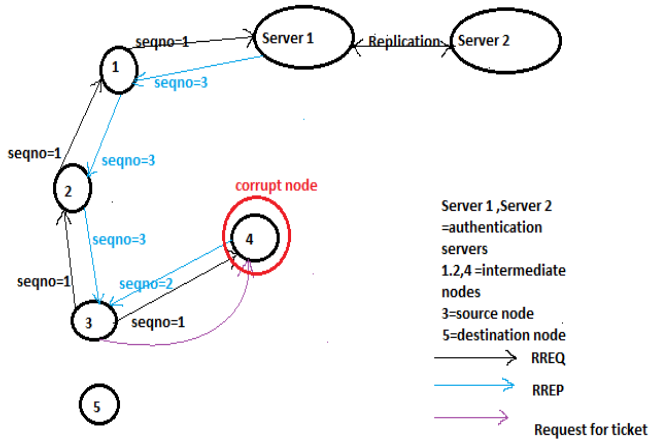

Fig 4: Black hole attack in Kaman

6. Conclusions and Future Work

In this paper we conclude that when Kaman will be implemented in larger network, some routing protocol is needed for routing the packets, here we have used AODV reactive routing protocol .Which opened room for the black hole problem. This work can be extended to fix this problem and can be used for the networks with much wider domain using Kaman model.

7. ACKNOWLEDGEMENTS

I thank my guide Ms. Rupinder Kaur Cheema. Her guidance and support, and her understanding were a valuable asset

during the research. I thanks for her unconditional support, for inspiring me, for her valuable insights, patience and guidance. I am very honoured to have had the opportunity to work with her. I specially thank to my parents who helped me a lot during this work.

8. REFERENCES

[1] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan : Mitigation of Black Hole Attacks for AODV Routing Protocol

[2] Celia Li and Uyen Trang Nguyen: FAST AUTHENTICATION FOR MOBILE CLIENTS IN WIRELESS MESH NETWORKS

[3] Kimaya Sanzgiri,Bridget Dahill,Brian Neil Levine,Clay Shields,Elizabeth M. Belding-Royer: A Secure Routing Protocol for Ad Hoc Networks

[4]. Lidong Zhou, Zygmunt J. Haas: Securing Ad Hoc Networks

[5]. Asad Amir Pirzada and Chris McDonald: Kerberos Assisted Authentication in Mobile Ad-hoc Networks

[6.] Sang-Gon Lee: Cryptanalysis of Multiple-Server Password-Authenticated Key Agreement Schemes Using Smart Cards

[7] Yixin Jiang, Chuang Lin,Senior Member, IEEE,Xuemin (Sherman) Shen,Senior Member, IEEE,and Minghui Shi: Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks