Modification in the Kerberos Assisted Authentication in Mobile Ad-Hoc Networks to Prevent Black Hole Attack

Manpreet Kaur  
M Tech Scholar(C.S.E)  
Amritsar College of Engineering & Technology  
Amritsar, India.

Tanu Preet Singh  
H.O.D(C.S.E)  
Amritsar College of Engineering & Technology  
Amritsar, India.

Barjinder Singh  
Lecturer(C.S.E)  
Lovely Professional University  
Jalandhar, India.

ABSTRACT
MANET is the self-configuring type of network in which the mobile nodes can leave or join the network when they want. MANET is decentralized type of network, no central controller is present. Due to their unique features mobile ad hoc networks can be deployed anywhere round the clock. 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 and added the concept of timers in KAMAN to solve the problem of black hole attack that aroused when Kaman protocol is embedded into large network AODV, on-demand routing protocol had been used to select secure shortest path between the nodes.

Keywords
Black hole, Mutual Authentication, Secure server, MANET, KAMAN.

1. INTRODUCTION
Mobile Ad Hoc Network consists of wireless mobile nodes where each node acts as a router that forwards the packets from one node to another node. In MANET nodes are free to move and hence topology of MANET is very dynamic. Such characteristics allow an ad hoc network to be established on the fly with built in fault tolerance and unconstrained connectivity. This makes routing in such networks more challenging, especially when certain Quality of Service requirements are to be guaranteed during the routing. There is no fixed infrastructure in the MANET therefore each node must cooperate for forwarding the packet from source node to destination node. To form such a cooperative and self-configurable environment, every mobile host must be willing to relay messages from other hosts to their ultimate destinations. In such a network, it may be necessary for one mobile host to enlist the other hosts in forwarding a packet to its destination, due to the limited range of each mobile host’s wireless transmissions. This type of wireless network is known as mobile ad hoc network. If there are only two hosts in the mobile ad hoc network then we cannot see the real routing process involved in the MANET. In many ad hoc networks, though, two hosts that want to communicate may not be within wireless transmission range of each other, but could communicate if other hosts between them also participating in the ad hoc network are willing to forward packets for them. To establish efficient direct or indirect 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.

Mutual 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 indirect authentication incorporated the use of third party. Authentication scheme proposed in the Kerberos authentication is a hybrid type of authentication scheme. Kerberos scheme is the combination of indirect and direct authentication.

2. LITERATURE REVIEW
Asad Amir Pirzada and Chris Kaman, 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 migrates a number of features from the traditional, wired Kerberos environments to the ad-hoc environment, including the prevention of node identity forgery, the detection of replay attacks, establishment of secure channels, mutual endpoint authentication, and the secure distribution of provisional session keys amongst replicated servers.[1] Kerberos tickets used in KAMAN authentication scheme can be captured over the network are prone to replay attacks. Modification in KAMAN protocol can increase authorization. All of contents are encapsulated in an encrypted packet. So the replay attacks become impossible. To prevent reply attack they add session parameter in the Ticket grand message [2]. Semih Dokurer and Y. M. Erten and Can Erkin Acar investigated the effects of black hole attack on the network performance. A wireless ad-hoc network is a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad-hoc networks may be unprotected against attacks by the malicious nodes [3]. Failures may cause data packets to be silently dropped inside the network without triggering any alarms or responses (e.g., the failure is not routed around). So-called “silent failures” or “black holes” represent a critical threat to today’s rapidly evolving networks. In this paper, we present a simple and effective method to detect and diagnose such silent failures. Our method uses active measurement between edge routers to raise alarms whenever end to end connectivity is disrupted, regardless of the cause. These alarms feed localization agents that employ spatial correlation techniques to isolate the root-cause of failure [4]. Black hole attacks occur when an adversary captures and re-programs a set of nodes in the
network to block/drop the packets they receive/generate instead of forwarding them towards the base station. As a result any information that enters the black hole region is captured. Black hole attacks are easy to constitute and they are capable of undermining network effectiveness by partitioning the network, such that important event information do not reach the base stations. In this paper, they may even end up making black hole attacks more effective. We propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on the data transmission [5].

3. KERBEROS ASSISTED AUTHENTICATION PROTOCOL IN MOBILE AD HOC NETWORKS

Kerberos assisted authentication protocol is the extension of traditional Kerberos authentication protocol. 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 assisted authentication protocol eliminates various disadvantages of traditional Kerberos authentication protocol. As much numbers of message is needed for successful authentication which leads to degrade the battery performance of the mobile devices. In KAMAN only two parties are involved while authentication but in traditional Kerberos protocol third party had involve while authentication. The third, main disadvantage of traditional Kerberos protocol is the assumptions that we assume while implementing the protocol in the actual environment when the environment in which Kerberos protocol is embedded change Kerberos protocols performance factors degrades. We assume while implementing the protocol in the actual environment when the environment in which Kerberos protocol is embedded change Kerberos protocols performance factors degrades.

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 secret key Repository are encrypted with the secret key when replication takes place.

![Figure 1: Operations of kaman](image)

Suppose two mobile nodes are node 1 and node 2. Server1 and server 2 are the authentication servers. When mobile node1 wants to communicate with node 2. Node1 and node 2 should be mutually authenticated with the authentication server. For authentication, node 1 requests for a ticket to server 1. When node 1 has been successfully authenticated, server 1 sends ticket to node 1. Ticket contains the virtual ids of node 1 and node 2. Shared key communication between node 1 and node 2 is encrypted with shared key and tickets are encrypted with public key of node 1. When node 1 receives ticket, it decrypts the ticket with its own private key and encrypts the same ticket with the public key of node 2. When node 2 receives, ticket from node 1, it will decrypt that ticket with its own private key. After receiving the ticket, node 2 sends acknowledgment to node 1. On receiving the acknowledgment node 1, starts the communication with node 2. The servers, server 1 and server 2 have been replicated. In KAMAN we will assume that hashed passwords are stored on the authentication servers and each server is mutually authenticated with other server.

4. PROPOSED WORK

This work is about wireless ad hoc networks. The purpose of this work is to promote the secure and reliable data transmission. It has been attained by the use of Kerberos assisted authentication protocol with multipath routing AODV protocol. Kerberos assisted authentication protocol have been used for the mutual authentication, to maintain the trust relationship between the mobile nodes and multipath routing protocol AODV for fast data transmission. Here our work is based on two methods

- Kerberos assisted authentication protocol
- Multiple routing protocol AODV

We are implementing the KAMAN model in large network and embedded AODV routing protocol with the same. The network had been set up with finite number of nodes and servers, along with defining the source and destination nodes. By using AODV routing protocol, source chooses the shortest path between source and server. Source wishes to communicate with destination. So prior to communication, there must be mutual authentication established between the two parties. For mutual authentication, source requests to its nearest server. The source sets the threshold value of timer. If source gets the ticket within threshold value, then sends the same to the destination for mutual authentication. If not, the source has to change its path, as Black hole has been triggered and it drops the ticket. So, source has to make the request to the server for ticket again. When source gets successfully authenticated to Server, Server then issues Ticket to source. If the ticket is successfully received by the source afterwards, source passes that Ticket to destination. When destination receives, the Ticket it sends the acknowledgement to source. Ticket contains the shared key which is generated by the Server. Data exchanged between source and destination 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.
5. **RESEARCH METHODOLOGY**

![Flow Chart of Proposed Work](image)

**Figure 2:** Flow Chart of Proposed Work

6. **SIMULATION RESULTS**

**Figure 3:** network deployment

The network is deployed with the finite number of mobile nodes. In the deployed network some mobile nodes become server on the basis of usage.

**Figure 4:** Server formation

The certain mobile are formed as the servers. The nodes are formed as servers on the basis of usage. The hash passwords of the mobile nodes are stored on the servers.

**Figure 5:** Route request packets flooding

The source nodes flood the route request packets in the network. The intermediate nodes which is having path to server will reply back with the route reply packets.

**Figure 6:** Best Path Selection

The source node selects the best path to destination on the basis of hop counts and sequence number. The route which is having minimum number of hop counts and higher sequence number is selected as best route.
When the route is established between source and server, source requests for the ticket.

The source node requests for ticket to server. In the route which is between source and server in this route some malicious nodes can exists. The malicious nodes are responsible for triggering the black hole attack. The malicious node keep on dropping the packets and source will wait for ticket.

When source is not able to get ticket for threshold period of time, it changes its path and selects the second best path. Through the second path source request for the ticket.

When the source node gets ticket through the second best path, the communication starts between source and destination.

7. COMPARISON GRAPHS

7.1 Delay

The y axis of the graph represents the number of packets and x axis represents the time. The delay in previous technique is maximum due to black hole problem. In novel approach delay will be constant for certain period of time, and then take hike to certain constant value.

7.2 Energy

It can be seen from the graph that energy has been increasing with the increase in the number of packets. There has been a considerable hike in the amount of energy increased, if we compare the statistics of the previous and novel technique.

7.3 Throughput


[17] Georgios Kambourakis, Elisavet Konstantinou,” Efficient Certification Path Discovery for MANET”.


