iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Novel SAT KAMAN protocol to prevent DOS attacks in MANET

Simranpreet Singh Chhatwal[1], Manmohan Sharma[2]
Student M.Tech (IT), Assistant Professor
Department of computer science, Lovely Professional University, Phagwara, India

Abstract- The Kerberos assisted authentication protocol is the efficient protocol that have been used for this identity validation. Kaman is the extension of Kerberos protocol with the use of Kaman nodes in the ad hoc network are authenticated by the secure server. SAT KAMAN means secure, acknowledge and timer based KAMAN. This can caused for 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 work, the Kaman (Kerberos assisted Authentication in Mobile Ad hoc Network) model has been analysed for the existing loopholes. Black hole attack that aroused when Kaman protocol is embedded into large network has been worked upon, by the incorporation of the timers. AODV, on-demand routing protocol had been used to select the secure small path and node communicate with an authenticated server for mutual authentication, optimal path will be selected by the virtue of the proposed methodology. Thus, it ensures the secure communication establishment in case of mobile ad hoc networks. Hence the network performance has been upgraded.
Keywords- MANET, Malicious node, Black hole node, KAMAN, AODV

I. INTRODUCTION

Wireless network technically, refers to the category of networks in which intercommunication between nodes is implemented without the use of wires. Wireless networks use radio waves and microwaves to establish communication between the devices. Wireless networks have following advantages over wired networks:

- Easy to deploy and initial cost of deployment is less.
- Wireless networks are more flexible and can easily adapt to changes, when environment in which network is to be established and configured changes.

Wireless networks can be extended to the places, where the use of wires is not feasible. Wireless networks can be classified in two types:-

- Infrastructure based network.
- Infrastructure less network.

II. KERBEROS PROTOCOL

Kerberos is the network authentication protocol and it provides strong authentication to the clients and servers [1]. Kerberos protocol facilitates secure communication between the clients and servers by the incorporation of a secret-shared key. The client, when wishes to communicate with the server, has to authenticate itself to the server. While proving its identity, client has been sharing its password to the server. Once the password has been matched and correctly client will successfully authenticated. If the passwords are unencrypted, then attacker can simply sniff the network traffic and get the access to the passwords of the legitimate clients. When illegitimate client gets the password of the legitimate client, it can use it whatever way he wish to. Kerberos protocol provides imbuement of encryption in the passwords. The legitimate client prior to the establishment of the authentication encrypts the password that has been used for validating identity. When client will be successfully authenticated with the server, all the communication between the client and server will be in the cipher text form. Consequently, data integrity and privacy has been ensured [1].

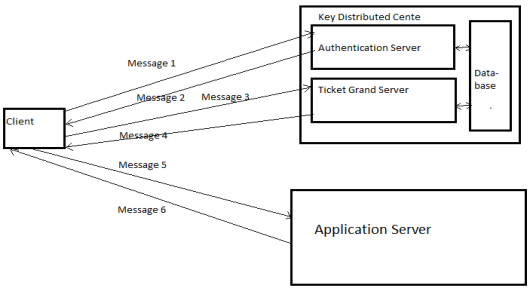


Figure 1: Kerberos Protocol operations

As, shown in the figure 1, when the client wants to successfully authenticate with the application server. It needs to get the hold of the ticket which it presents to the application server. For getting the ticket, client communicates with the key distributed center components. Authentication server and Ticket Grand server are the two components of Key Distributed Center. Following are the messages which are exchanged between the client, Key Distributed Center and Application Server for successful Authentication:-

A. *Message 1:* Client sends its identity to the Authentication server and requests for the ticket (TGT).
B. *Message 2:* When authentication server successfully validates the identity of the client. It provides the TGT to the client, which then decrypts the TGT with its own hash password.
C. *Message 3:* When client gets the TGT, it presents TGT to the ticket grand server to receive the service ticket.
D. *Message 4:* When Ticket grand server verifies the TGT, it provides the service ticket to the client.
E. *Message 5:* When client gets the service ticket, it then presents the service ticket to the application server for mutual authentication.
F. *Message 6:* When the client and server are mutually authenticated, server provides the session key for secure communication between two.

III. LITERATURE SURVEY

Assad Amir Prada et.al (2009): In this paper they had proposed a new mutual authentication scheme is Mobile ad hoc Network. Kerberos Assisted Authentication Scheme is the extension of tradition Kerberos version 5 Protocol. They had assumed that the hashed password of users is stored on the server and each server is mutually authenticated with other server. When any mobile node wants to communicate with the mobile node .Secure server provides shared key communication between the mobile nodes is encrypted with that shared key [2].

Kamarularifin Abd. et.al (2010): In this paper they had discuss details of AODV (ad hoc on demand vector) protocol that how secure and efficient route is selected for data transmission. They had also discussed black hole problem which arises in AODV protocol. They had proposed scheme for migrating black hole problem in AODV protocol .The proposed scheme is named as ERDA scheme and in this scheme receivreply() fuction is updated [4].

Adebanjo Adekiigbe, et.al (2011): In this paper they had review the cluster based scheme to remove congestion in wireless mesh Network. When available are less and demand of resources are more then congestion occurs. To solve the problem of congestion clustering scheme is proposed [3]. All the nodes choose their cluster head and the entire nodes share their resource with the cluster head. In this paper they had also discuss various clustering algorithms to choose cluster head.

Nisha P John, et.al (2012) discussed mobile nodes form temporary ad hoc network that is dynamically and infrastructure less. To protect the ad hoc network we are using many firewalls and encryption algorithms. But it is not sufficient due to limited resources and mobility. Our main goal is to provide the security services such as authentication, integrity, availability and confidentially to mobile users. In ad hoc networks, Black hole attack is easily employed by exploiting vulnerability of AODV[5].

IV. PROPOSED SCHEME FOR THE ATTACK DETECTION

MANET is a self-configured type of network it means any node can join it or leave it at any time. So nodes are changing during time to time so it has a synchronization between nodes and server so that every node can store key inside server which is required for ticket granting. If a malicious node exists during synchronization in between nodes and server then it will drop data and server will never synchronize with nodes. So to remover these kind of DoS attacks we are proposing a scenario which is based on symmetric, asymmetric, timer and acknowledgement based.

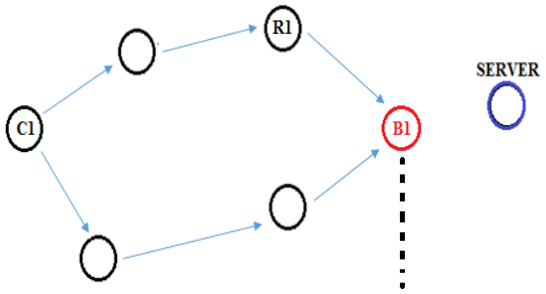


Figure 2: Attack in KANAN schema

Here nodes are strongly synchronized using symmetric and asymmetric key cryptography techniques and the cross checking is done on the basis of timer and ACK

Authentication steps of proposed schema:

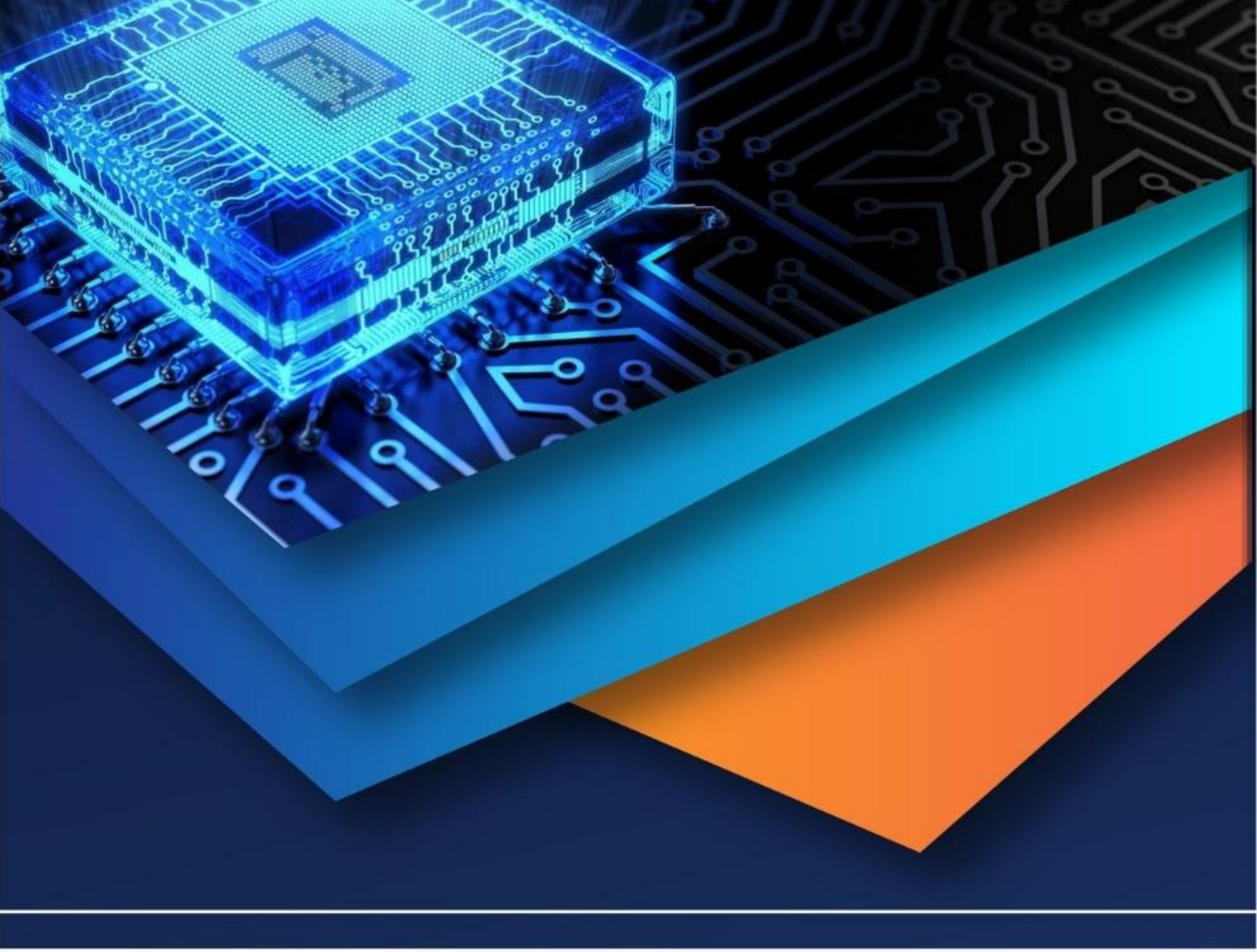
A. PUB_{key} ➔ Node: Server broadcast its public key
B. $E(PRI_{key})$ ➔ Server: All nodes encrypt there private key with public key of server and send to server.
C. If (Server receive all keys = communication done) else
D. Timer: server wait till timer gets expired if it will not receive any key.
E. If the network have black hole node then it will drop all packets.
F. Isolate last node of path because it is the one who is responsible for packet drop because black hole node is always exist on last of path because it never forward data.
G. Server broadcast message to send key again.
H. Nodes send keys again. This time server receiver keys because black hole node is isolated.
I. SERVER ➔ $NODES_{MSG}$: Server receive all keys.
J. Client request to server.
K. Request for path till R1.
L. If there is new black hole node join network and it reply for path.
M. Set Timer at R1.
N. R1 alert C1 that he is not getting any data.
O. Isolate new black hole node.
P. Send data through path from where C1 receive ACK from R1.

V. CONCLUSION

In our work, 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. The black hole problem is solved with the user of timer in KAMAN. Timer is embedded into KAMAN, which will expire after threshold period of timer. In fixed threshold period of timer, if source unable to get ticket from secure server automatically source select another best route for communication with secure server.

REFERENCES

[1]. Asad Amir Pirzada and Chris McDonald," Kerberos Assisted Authentication in Mobile Ad-hoc Networks" School of Computer Science & Software Engineering, The University of Western Australia 35 Stirling Highway, Crawley, W.A. 6009, Australia.
[2]. Adebanjo Adekiigbe, ,Kamalrulnizam Abu Bakar And Ogunnusi Olumide Simeon (2011), "A Review of Cluster-Based Congestion Control Protocols in Wireless Mesh Networks",1 IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011 ISSN (Online): 1694-0814
[3]. Kamarularifin Abd. Jalil , Zaid Ahmad , Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol", Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Malaysia, Shah Alam, Selangor, Malaysia.
[4]. Mr. S. K. Pathan, Mr. S. N. Deshmukh, (2009), "Kerberos Authentication System – A Public Key Extension", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009
[5]. Nisha P John, Ashly Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review", International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 ISSN 2250-3153



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY