International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 6 ǁ June. 2013 ǁ PP.42-47

Attack Library Based Intrusion Detection System to Secure Manets

Shashank Kumar Chaudhary [1],Bramah Hazela [2]

([1] Department of computer science and engineering, Amity University, Lucknow, India)
([2] Assistant Professor, Department of computer science and engineering, Amity University, Lucknow, India)

ABSTRACT: *A mobile ad hoc network is a wireless network which is also infrastructure less network, these networks are self-configuring. Due to lack of infrastructure and central management, the security issues are the important concern. In this paper author have proposed a model which provides certificate based authentication and attack library based Intrusion detection system. Certificate based authentication helps to establish a secure connection, whereas attack library based intrusion detection system provide facility to detect the malicious node present in the network.*

KEYWORDS: *Dynamic certificate Authority, Intrusion Detection System, mobile ad hoc networks***.**

I. INTRODUCTION

A mobile ad hoc networks are the wireless network with the collection of mobile nodes. The mobile nodes are connected in to each other during communication .The mobile nodes in the network can move up to a range during the communication. The intermediate mobile nodes in the network act as the mobile agent. The mobile nodes in the MANETs may be with bi-directional or unidirectional links .Each node in the network act as the router, transmitter or receiver. The mobile nodes operate in the network because they have their individual battery power.

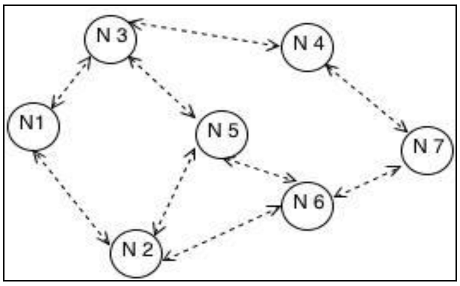

Fig.1 Mobile ad hoc network.

MANET follows different mobility models according to their temporal and spatial dependencies. Mobility models used are: random waypoint, random point group mobility and freeway mobility model. Due to the mobility of nodes the routing protocol performance affected. Due to the rapid growth of mobile gadgets such as laptop, mobile phones, PDAs etc., MANET become the communication paradigm. Infrastructure network based on the fixed base station which acts as access point (centralized point). Infrastructure less network are wireless network, they are self-configuring so there is no centralized access point. MANETs was designed for military application, natural disasters, data collection and virtual classes. MANETs are categories in two types: open manet and closed manet. In open manet resources are shared among nodes to achieve different goal. In closed manet resources are shared among nodes to achieve common goals .Security has become important issue in the MANETs. Attacks in the adhoc network due to the presence of the malicious node. In this paper, MANET security issue is tackled, namely to prevent the network from malicious node and to establish a secure communication between the secure nodes.

II. BACKGROUND

MANET is a self-organizing network of mobile nodes. MANET does not have any fixed topology, due to dynamic topology it is very difficult task to secure network topology. Several papers focused on the security issues of the MANET.

D. Sterne, et al. [9], described a architecture for intrusion detection to secure MANET. The architecture works in hierarchy it collects the detection data from leaves node and flow upward to the root node. To establish a secure communication, the hierarchy automatically reconfigured itself based on network topology. A new intrusion detection system name Enhanced Adaptive Acknowledgement (EAACK) was proposed by U. Sharmila Begam,et al. [1].

EAACK is able to detect the malicious node based on report of misbehaving node. While detecting malicious node, the EAACK does not affect network performance. S.Tamilarasan, et al. [5] describe the logical survey to detect the malicious node based on their behaviour and pattern, and proposed the techniques used for detecting misbehaving nodes. To establish a trust management by monitoring the other neighbor nodes Reijo Savola [8] has proposed a model, and also describe the security metrices used in MANET.

III. PROBLEM DOMAIN

In many research work different techniques have been proposed for detecting misbehaving nodes. Detecting misbehaving node through proposed techniques is a time consuming process. These techniques are time consuming because they are applied one by one to detect misbehaving node. To overcome this problem author have proposed an attack library based intrusion detection system. Dynamic certificate authority based authentication model is proposed to establish a secure communication between the nodes.

IV. BEHAVIORAL CHARACTERISTICS OF NODE IN MANETS

In MANET nodes act as receiver and transmitter within communication range. Source node communicates to destination node through intermediate nodes present in the network. Attacker aims to attack the network through these intermediate nodes by making these nodes malicious.
Malicious nodes tend to cause fallowing attacks:

A.) Black-Hole Attack

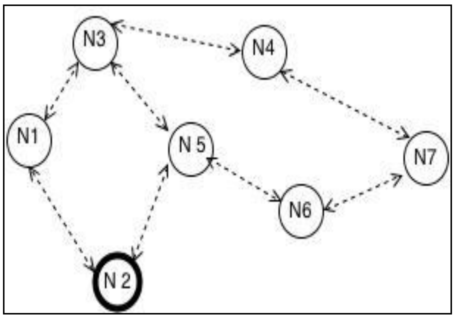

Fig.2 Black hole attack.

In this attack the malicious node advertise or shows itself, having the shortest path to the destination node whose packets it wants to hamper. For e.g. in the above figure N2 (malicious node) in the network advertise itself to have shortest path to the destination node. So N2 node wants to interrupt destination node packet.

B. Worm-Hole Attack

The attacker creates a tunnel at malicious node so that when malicious node receives a packet it drops the packet through tunnel.

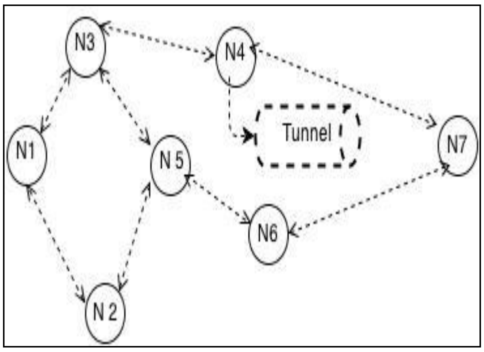

Fig.3 Worm hole attack.

For e.g. in the above figure the node N4 (Malicious node) creates a tunnel. When node N4 receives a packet then it drops through the tunnel.

C. Spoofing Attack

Misbehaving node hires the identity of another node and receives all the packets or messages of that node.

D. Denial of Service

The attacker node exploits the bandwidth of the network .The attacker node (malicious node) generates unnecessary route requests so that to make network resources unavailable to authentic nodes.

E. Energy Consumption

Mobile nodes in MANETs have limited battery backup. So the mobile nodes save their battery power by transmitting only necessary data. In this attack, attacker aims to consume the power of battery by routing unnecessary packets to other nodes.

F. Information Disclosure

In MANETs the data flow in the network in the form of packets. When the data is processed information is produced. In this attack the attacker attempts to destroy the confidentiality, integrity or availability of the data.

- ***Attacks on confidentiality***:

The attacker aims to disclose the confidential data of the data packet, which is only accessible by the authorized node.

- ***Attacks on integrity***:

The integrity of the packet is lost. The attacker, alter the data packets by modification and removal of data packet content.

- ***Attacks on availability:***

In this attack the attacker node routes huge amount of unnecessary traffic to make network resources unavailable to other nodes.

V. INTRUSION DETECTION SYSTEM (IDS)

In any network intrusion detection system (IDS) monitors activities of both user and program. Intrusion detection can be done in two ways: Network based intrusion detection and Host based intrusion detection. Network based intrusion detection runs at the gateway of the network and monitor and captures all the information about packet that passes through that gateway whereas host based intrusion detection system runs on the operating system and monitors all the program and event performed by the user or host.

A. Attack Library Based Intrusion Detection System

An attack library is the collection of types and patterns of attacks. Varying components of attack library based intrusion detection system are as follows:

- ***Analyzer:***

The work of analyzer is to analyze and monitor the node in the network. Analyzer fallows two methodologies for detection: misuse and anomaly detection.

Misuse detection is based on the pattern, in this detection the node pattern in terms of their event sequence is monitor. Anomaly detection is based on the behavior monitoring, the node behavior deviations is compared with normal behavior, if there is change then the analyzer record it.

- ***Attack Library:***

Attack library is a collection of well-organized designed attacks and test cases. It also provides facility to generate new test cases for new attacks. Attacks are organized in the hierarchy structure. The attack library uses these patterns and behavior to construct the test cases. The attack library works on a step of designed test cases. The attack library generates response on the given input. It also generates the UID (unique ID) for the authentic node. Attack library also monitors the behavior and pattern of directly attached node.

- ***Certificate Authority:***

Certificate authority is the trusted authority that can be used for issuing certificate to make secure communication .The certificate consists of UID, block signed by certificate authority, Key .UID in the certificate is generated by the attack library after verification of node that it is not a malicious node.

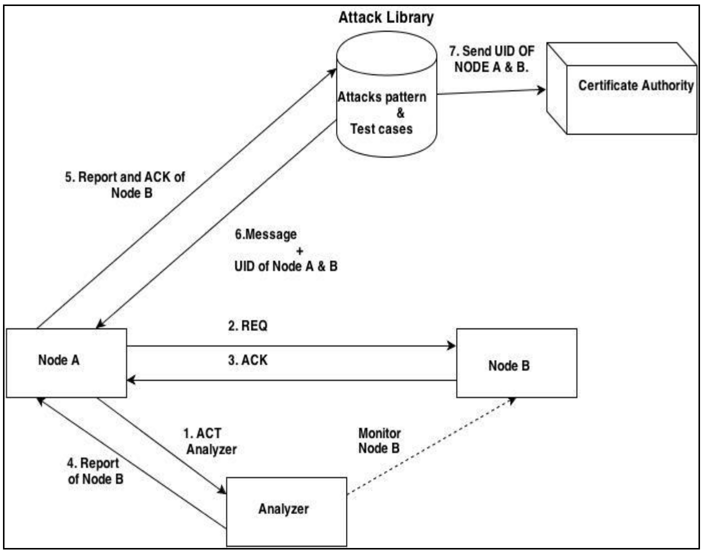

Fig.4 Attack Library based intrusion detection system

Steps involved in attack library based intrusion detection system are:

1. Node A activates the analyzer with information to monitor node B.
2. Node A sends a request to node B to establish a communication path.
3. Node B send acknowledgement to node A. Node B send acknowledgement to ensure that he has received the request. Node B sends a message with acknowledgement whether he wants to establish a connection or not.
4. Analyzer analyzing Node B during the step-2 & 3. Analyzer sends report of Node B to Node A.
5. Node A sends report and acknowledgement of node B. Node A sends ACK of Node B because it contains network parameters like response time etc.
6. Attack library response with a message and UID (unique ID) of both nodes A & B. Message contains information about node B where it is a malicious node or not. The UID is generated by attack library only when the node is not a malicious node. If it is malicious then Node A broadcast a message in the network that Node b is malicious. Here attack library monitor node A (direct attached to attack library) after getting report and acknowledgement of node B. Attack library monitor requesting node (node A) to check it is malicious or not.
7. Sends UID to certificate authority

VI. DYNAMIC CERTIFICATE AUTHORITY BASED AUTHENTICATION

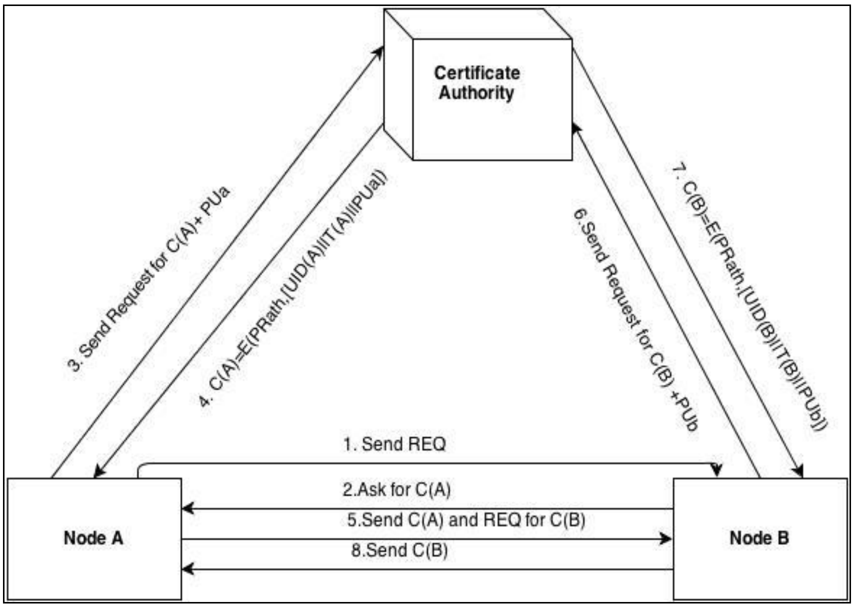
Certificate Authority
3. Send Request for C(A)+ PUa
4. C(A)=E(PRath,[UID(A)||T(A)||PUa])
6.Send Request for C(B) +PUb
7. C(B)=E(PRath,[UID(B)||T(B)||PUb])
1. Send REQ
2.Ask for C(A)
5.Send C(A) and REQ for C(B)
8.Send C(B)
Node A
Node B

Fig.5 Dynamic Certificate Authority.

Dynamic certificate authority is the collection of node UID and its work is to issue certificate to establish a secure communication between the nodes. The UID is used by certificate authority during issuing certificate. UID is generated by the attack library during intrusion detection. Due to the concept of attack library based UID generation only authorized nodes in the network can request for a certificate from certificate authority. In the above diagram C(A) is certificate of node A, C(B) is certificate of node B, PRath is private key of certificate authority, T(A) is time stamp for node A certificate, T(B) is the time stamp for node B certificate, PUa and PUb are the public key of node A and B. Steps involved in Dynamic certificate authority to issue a certificate are:

1. Node A sends a request to node B to establish a connection.
2. Node B asks for certificate from Node A.
3. Node A send request to certificate Authority to generate certificate of node A and also send public key of A.
4. Certificate authority send certificate to node A which includes UID, Time stamp of node A and public key of A. The certificate is encrypted by certificate authority using its own private key.
5. Node A receives certificate and decrypt certificate using the public key of certificate authority. Node A checks for time stamp T (A) to conform that the certificate is not old. Then send C (A) to node B and request for B certificate.
6. Then node B send request to certificate authority to generate certificate C (B) and also sends his own public key PUb .
7. Certificate authority generates certificate and encrypt with its own private key and send to node B.
8. Node B decrypts certificate using public key of certificate authority and checks time stamp. Then node B send certificate C (B) to node A.

After exchanging certificate of each other node A and node B can establish a secure communication.

In proposed model Dynamic certificate Authority the name dynamic is used because the certificate authority database is transfer to another authentic node present in the network. The certificate authority maintains a priority list of nodes on the basis of number of times the node has requested for the certificate. The certificate authority selects that node which has less time requested for certificate because that node power energy backup is more than the other busy nodes present in network.

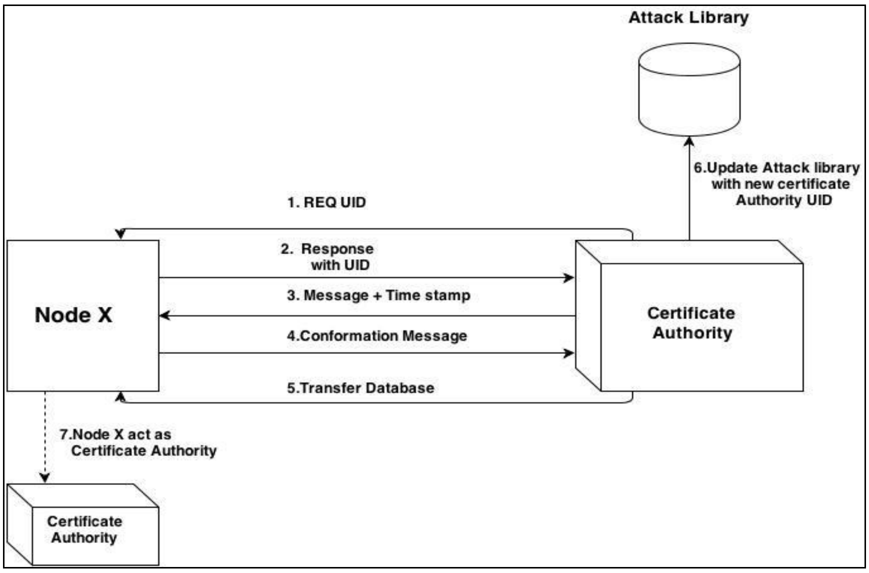

Fig.6 Transfer of certificate authority database.

1. Steps involved during the transfer of certificate authority database are:
2. Certificate authority selects the node from priority list to which he wants to transfer the certificate authority database. After selecting the node certificate authority send request for UID of node X.
3. The node X response to the request and send UID to certificate authority.
4. Certificate authority checks for the UID and conform that the node is authentic or correct one. Then certificate authority send a message to node X which include that he wants to establish a connection and attach a time stamp that is used maintain a session for given period of time.
5. Node X sends conformation message.
6. Certificate authority transfer database to node X.
7. Certificate authority update attack library with the UID of new certificate authority.
8. After all these process the Node X acts as the new certificate authority.

VII. CONCLUSION

This paper focuses on security measures to secure MANETs from attacker. The proposed model which is based on Attack library based intrusion detection system, helps in detecting the malicious node to secure the network. Further dynamic certificate authority based authentication model have been proposed which is used to make an trusted communication between the nodes by using exchanging certificate.

VIII. FUTURE SCOPE

Many research has been done and going on the security of MANET. Moreover the proposed security model is used to detect the malicious node and to make a secure communication. Our future work will include the further exploration of attack library i.e. patterns, test cases and to implement the proposed model using simulator.

IX. ACKNOWLEDGMENT

I would like to thanks Maj. K.K. Ohri (AVSM), Pro.V.C, Amity University, Lucknow Campus. I would like to further extend my sincere gratitude to Prof. S.T.H. Abdi, Director(ASET) , and Brig. Umesh Chopra, Deputy Director (ASET), Amity University, Lucknow Campus for their encouragement. I am extremely grateful to Prof.Deepak Arora, head of computer science and engineering department for this insightful comment. I would like to express my sincere thanks to Bramah Hazela , Assistant professor , Department of computer science and engineering ,Amity University Lucknow.

REFERENCES

[1]. U. SharmilaBegam, Dr. G. Murugaboopathi, “A RECENT SECURE INTRUSION DETECTION SYSTEM FOR MANETS” in International Journal of Emerging Technology and Advanced Engineering Volume 3, Special Issue 1, January 2013.

[2]. DilipVishwakarma, Deepak Chopra, “International Journal of Engineering and Advanced Technology” in Volume-1, Issue-6, August 2012.

[3]. Mohammed Mujeeb, Sudhakar K N, JitendranathMungara, “Reputation-Based Security Protocol for MANETs” in International Journal of Innovative Technology and Exploring EngineeringVolume-1, Issue-2, July 2012.

[4]. Chandreyee Chowdhury, SarmisthaNeogy, “SECURING MOBILE AGENTS IN MANET AGAINST ATTACKS USING TRUST” in International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[5]. S. Tamilarasan and Dr. Aramudan, “A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System” in International Journal of Computer 258 Science and Network Security, VOL.11 No.5, May 2011.

[6]. N.Jaisankar, K.DuraiSwamy “A Novel security framework for protecting Network Layer operations in MANET” in International Journal of Engineering and Technology Vol.1,No.5,December, 2009.

[7]. S. Madhavi, Dr. Tai Hoon Kim, “AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOCNETWORKS” in International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[8]. Reijo Savola, “Node-Level Information Security Monitoring for Mobile Ad Hoc Networks” in Proceedings of the ETRICS'06 Workshop on Security in Autonomous Systems, 2006.

[9]. D. Sterne, P. Balasubramanyam, D. Carman1, B. Wilson, R. Talpade, C. Ko,R. Balupari, C-Y. Tseng2, T. Bowen, K. Levitt and J. Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs” in Third IEEE International Workshop on Information Assurance ,2005.

[10]. RicardoPuttini, Rafael de Sousa, LudovicMé, “Combining Certification-based Authentication and Intrusion Detection toSecure Manet Routing Protocols” in Proceedings of the European Wireless Conference Mobile and Wireless Systems Beyond 3G ,2004.

[11]. Y. Huang and W. Lee, “A cooperative intrusion detection system for ad hoc networks,” in Proc. ACM Workshop onSecurity in Ad Hoc and Sensor Networks (SASN'03),October 2003.

[12]. S. Capkun, L. Buttyan, and J. P. Hubaux.“Self-organized public key management for mobile ad hoc networks” in IEEE Transactions on Mobile Computing, page 17, 2003.