International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Security for Mobile ADHOC Network using Intrusion Detection System

Roopa Lakshmi S[#1], Anusha V G[*2], Anushree S A[#3], Gowthami B S[#4], Chaithra T S[#5]
[2,3] *Asst Professor/CSE,* [1,4,5] *UG students/CSE*
Vemana Institute of Technology, #1, Mahayogi Vemana road, 3rd Block,
Koramangala, Bangalore-560039, India

***Abstract* — By a collection of mobile nodes mobile adhoc network are self-created and self-organized, used to exchange information as a wireless adhoc network and multi-hop wireless paths are interdependent. In present locality MANET has become a key mechanization. Mobile hand held devices like cell phones, laptops, PDA etc forms MANET. MANET are very useful in the situations like military operations and emergency management as MANET is used in crucial situations, so concern for security is more. MANET is dynamic in nature and lack in centralized monitoring points which results in vulnerable attacks.**

***Keywords* : Adhoc networks, attacks, security.**

I. INTRODUCTION

The self-configuring infrastructure less network forms a MANET of mobile portable devices combined by wireless connectives. The control of every device in MANET is not under control of another device to move unrestrictedly in any order and change its links to other devices regularly. MANET is suitable in situations like natural calamities like flood, earthquake or hilly terrain and military war. MANET has major issues such as lack of fixed infrastructure, backup power, mobility as well as security. Every node has to perform as a sender as well as receiver for communication. MANET have to resolve themselves if there is any conflicts like self-service, entry of external group or individual and in case of any failures .

A. ATTACKS (OR) EXPLOITS

Attacks are classified into various types based on their behavior.

- **PASSIVE ATTACK**

The open ports and vulnerabilities are scanned and monitored in a passive attack which is also a network attack. All incoming and outgoing service of network is analysed in passive attacked but not renovated or modified. Passive attacks are not very virulent.

TABLE I.

TYPES OF ATTACKS	NAME OF ATTACKS
PASSIVE ATTACK	TAPPING SCANNING ENCRYPTION TRAFFIC ANALYSIS

Tapping: Monitoring unencrypted communications such as email or phone calls.
Scanning: Scanning a agent linked to the internet for obligations such as an uncertain operating system variant or open storage.
Encryption: Trying to crack the encryption and Preventing encrypted knowledge flows.
Traffic Analysis: Monitoring internet traffic to build data such as who is visiting which website.

- **ACTIVE ATTACK**

A network exploit in which a hacker undertakes to make changes to data on the target or data along the way to the target is an active attack which is also a network attack. Active attacks are more dangerous compared to passive attack.

TABLE II.

TYPES OF ATTACKS	NAME OF ATTACKS
ACTIVE ATTACK	MASQUERADE REPLAY MODIFICATION OF MESSAGES DENIAL OF SERVICE.

Masquerade: When one entity acts to be a different entity masquerade takes place.

Replay: Replay is an attack in which service is already recognized and concluded is imitated by another corresponding request.
Modification of messages: Some legitimate message sections are altered or delayed or reordered to construct and unauthorized effect.
Denial of service: The normal use or management of communication facilities are prevented and inhibited.

B. INTRUSION DETECTION SYSTEM

A device or software application that supervises a network or systems for harmful activities or policy violation is an IDS. Many attributes are present in IDS such as:

HOST-BASED INTRUSION DETECTION SYSTEM: The first type of intrusion detection software was HIDS to be designed the mainframe computers with the original target system where outside interaction was unusual. An intrusion detection system HIDS on its network integration analyses and monitors the internals of a computer system as well as the network packets. HIDS have a major drawback that they sometimes falsely report for the intrusion into the system.

NETWORK-BASED INTRUSION DETECTION SYSTEM: To protect a system from network based threads Network-based IDS is used to monitor and analyze network traffic. All inbound packets and searches for any suspicious patterns are read by NIDS. The NIDS major drawback is that they can detect only those intrusions whose patterns or signatures are already stored into the intrusion database.

WE HAVE MANY OTHER CLASSIFICATIONS BASED ON WORKING OF IDS:

SIGNATURE-BASED IDS: The tracking of attacks by looking for a specific pattern is mentioned as Signature-based IDS. All known attacks can be easily detected by Signature-based IDS, to detect new attacks which has no pattern it is not possible.

ANAMOLY-BASED IDS: To track unspecified attacks in part due to the rapid expansion of malware Anamoly-based IDS were initiated. Anamoly-based approach enables the detection of previously unknown attacks.

MISUSE-BASED IDS: Misuse detection is an approach to detecting computer attacks. In a misuse detection approach, abnormal system behavior is defined first and then all other behavior is defined as normal.

MOBILE AGENT-BASED IDS: Distributed system with the characteristics such as mobility and autonomy uses Mobile agent-based IDS .Some other attributes of IDS are Log-based, Rule-based and Hybrid.

COMPONENTS OF IDS: Data Collector: The activities which are performed by the user on the local machine is collected by the Data Collector.

DETECTION ENGINE: By using some applicable intrusion detection algorithm it guarantees whether the system has intrusion or not.

ALARMING SYSTEM: The alarming system sends alarming message to all the nodes when detection engine assures that an attack has been penetrated into the system and then the alarming system alerts all the nodes about the intrusion. Among all the IDS, Signature based IDS will identify the intrusion only those signatures which match with the existing signatures in the database. Compared to other IDS signature-based IDS is better with respect to performance as it gives very less incorrect positive rate.

II. LITERATURE SURVEY

In [8] by using RSA algorithm the authenticity is ensured through access control. To identify the malicious activities, it makes use of threshold signature. In threshold signature nodes take part co-operatively in a distributed manner. So it is distributed process. An admissible threshold of malicious group members can completely recover the group RSA secret key in the lifetime certainly is shown in the proactive RSA scheme. This proactive RSA scheme has threshold signature protocol as its part which leaks information about the secret signature key. In [7] to find the selfish nodes into mobile adhoc networks, game theory model is used. In order to become intense possessor nodes may little egoistic. To apply the game theory the constants allowed are transmission, throughput and delay. This access control scheme has an advantage allowance of fair channel nodes which do not collaborate with each other and are selfish in competing for transmissions . In [9] it describes the unified methods to accomplish both privacy and authorization through access control and it is called here P+A where, P means privacy and A means access control. This scheme defines a kind of language to check access control and privacy it has some policies, constraints and axioms. In [11] to ensure the authenticity of the message in a wireless ambience it make use of protocol LWAC location based access control. To locate the mobile stations and access points it does not need the global poisoning system. To substantiate the location Diffie-Hellman (DH) key exchange algorithm is used. In [14] mobile adhoc networks are wireless networks that are dynamic in nature and lack in centralized monitoring points which results in vulnerable attacks. Monitoring capabilities are provided by IDS that help to identify the specific trust level and propose the local security to a node and other nodes. This effective communication between nodes in MANET's is done with the help of clustering mechanism where each cluster involves a number of member nodes which is managed by cluster head. To enhance the route efficiency the clustering mechanisms are generally used for the routing purpose. In [15] uses decision tree that is made on the basis of good features and bad features. Analysation of data and identification of significant characteristics can be done in decision tree which indicates malicious activities.

By analysing large set of intrusion detection data value to many real time security systems are added. Further investigation is supported by recognition of trends and patterns, attack signatures development and monitoring of other activities. Decision trees usage advantages instead of other classification techniques where a rich set of rules are provided which are easily understandable. In [18] by passing Hello message intrusion is detected co-operatively. Hello messages are used to maintain connectivity. In [19] to notice and validate the router in the network it uses the Chinese remainder theorem (CRT). So security attack can be substantiating the location of the source whether message has come from expected source or not to secure the originality. In the transmission process nodes involved are authenticates the threshold cryptography which is used to share the message and for routing verification Chinese Remainder Theorem and whether the node is authenticated or not is verified. In [17] filtering mechanism is used to refine out doubtful message before carrying them to the next node in the network. Each node receives the packet coming to it and checks for their authentication. It redirects the packet into the network after assuring that it is correct packet. To check the authenticity of received message each forwarding node is enabled by Filtering scheme and against attacks it acts as a protection. In [20] by decreasing the neighboring hops it narrates the energy efficient clustering. This scheme works in organization and cluster service design phases. In a set of clusters the MANET is divided into energy efficient and secure communication protocol where one cluster consists of each node. Each cluster elects a leader node (cluster head) among the nodes for the entire cluster to perform as the IDS.

III. PROPOSED METHODOLOGY

CLUSTER: To work as one centralized data processing resource through a dedicated network group of independent servers are interconnected. Mobile adhoc network appoints one of its nodes which will be coordinating with all other nodes of networks as the leader of clusters for decision making about the intrusion. In safe transmission way the cluster leader node collects information from all other nodes about suspicious attacks into the network and then this information will be sent to the global cluster head. Global cluster head is the main point where the final decisions will be made and transmitted to all nodes into the system. This global cluster head will report to all other nodes into the network whether there is an intrusion into the system or not at the end.

CRYPTOSYSTEM: A cryptosystem is also mentioned as a cipher system. An implementation of infrastructure and cryptography techniques is a cryptosystem to provide information security services.

COMPONENTS OF CRYPTOSYSTEM

PLAIN TEXT: During transmission the protected data is a plain text.

ENCRYPTION ALGORITHM: It is a cryptographic algorithm that takes plain text and an encryption key has input and produces a cipher text.

CIPHER TEXT: It is the scrambled version of the plain text produced by the encryption algorithm using a specific, the encryption key. Anyone who has access to the communication channel can be obstructed and adjusted.

Decryption algorithm: It is a cryptographic algorithm that takes a cipher text and a decryption key has input and outputs a plain text.

ENCRYPTION KEY: A key that is familiar to the sender is an encryption key. In order to evaluate cipher text the encryption key into the encryption algorithm along with the plain text is inserting by the sender.

DECRYPTION KEY: A key that is familiar to the receiver is a decryption key. In order to evaluate the plain text the decryption key into the decryption algorithm along with the cipher text is inserting by the receiver. In the system based on a manner in which encryption-decryption is carried out the cryptosystem is divided as following:

SYMMETRIC KEY ENCRYPTION: In the encryption process similar keys are used for encrypting and decrypting the information. Symmetric cryptography is known as study of symmetric cryptosystem and are also known as secret key cryptosystems. Digital Encryption Standard (DES), triple-DES (3DES) are examples for encryption of symmetric key.

ASYMMETRIC KEY ENCRYPTION: Various keys are used for encrypting and decrypting of the information in the encryption method. Pairs of dissimilar key, private key and public key should be present in the system. One key is used for encryption, the other key for decryption of cipher text back to the original plain text are mathematically interconnected. To insert the public key in public repository and private key as a well-guarded secret is required. Hence, this idea of encryption is also known as a public key encryption. Asymmetric key encryption in RSA has an example as shown below.

	SYMMETRIC CRYPTOSYSTEMS	ASYMMETRIC CRYPTOSYSTEMS
RELATION BETWEEN KEYS	SAME	DIFFERENT
ENCRYPTION KEY	SYMMETRIC	PUBLIC
DECRYPTION KEY	SYMMETRIC	PRIVATE

Every node has a key pair of public key and private key. Where, public key is familiar to each node in the domain and private keys are secret to all individual nodes in the domain. Public keys can be issued among all mobile nodes in one of the manners like publicly declaration, publicly key obtained directory, public key authority, public key certificate, public keys, Diffie-Hellman key exchange technique key distribution Centre (KDC) that divides a secret keys between every other node and itself. There secret are used to communicate with all the nodes by KDC. With the help of trusted KDC all received data is justified.

There is centralized key distribution Centre which has distributed public key pairs to every node into the cluster. Conversely, a key distribution centre has a cluster of leader. This leader knows the public key of all other nodes of the cluster and each node has its private key portion known to itself which is used for decryption and public key portion is used to encrypt the message to be transmitted. It installs local IDS and local data.

Structure of a node consists of Data Collection, Detection, Controller.
DATA COLLECTION: Data is collected by every node time to time on its local machine.
DETECTION: Intrusion is checked by pattern matching. If any new pattern is found this pattern will be sent to cluster leader in a secure way for further processing.
CONTROLLER: Communication between cluster nodes and itself is handled by this controller. To make the task more secure, controller deals with secure communication. Every cluster has a local cluster leader which is responsible for keeping an eye on intrusion or harmful activities into the clusters of the MANET. Global cluster head is also present that takes place of overall MANET and shares secret key with all other local cluster leader in the MANET. By sending messages time to time it communicates with other cluster leader.

SECURITY: The state of being free from anger or threat. The goals of security are Availability, Integrity, Authentication and Non-Repudiation.
AVAILABILITY: Nodes should be available for communication at all times. In despite attacks A node is needed to be continued to provide services.
INTEGRITY: The transmitted message is never misrepresented.
AUTHENTICATION: The distinctiveness of the peer node must be known which node it is communicating with. An attacker could interfere with other nodes and achieve sensitive information without authentication.
NON-REPUDIATION: The sender cannot dismiss sending of information and the receiver cannot dismiss the receiving of information.

IV. SYSTEM ARCHITECTURE

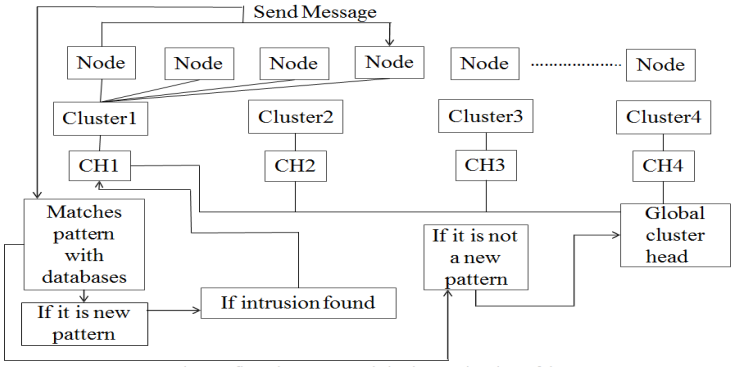

Fig.1:Defines the structure , behaviour and a view of the system

Mobile adhoc network designates one of its nodes as the leader of cluster because it will be coordinating with all other nodes of the network for making decision about the intrusion. This leader node will collect information about suspicious attacks into the network from all other nodes in secure transmission node. Then it will send this information to the global cluster head. This head is the main point and final decision will be made and communicated to all nodes into the system, by this it. At the end it will inform to all other nodes into the network whether or not there is an intrusion into the system. Users will set some rules for the nodes while analysing where nodes are patterns. These patterns will be sent to the database, if the pattern is matched or if it is a new pattern it will be sent to intrusion found which will be later directed to cluster hear where the information will be redirected to the global cluster head is the final decision maker which states as intrusion found. In another case, if it is not a new pattern it will be sent directly to global cluster head which states that intrusion is not found.

V. MODULE DESCRIPTION

NODE CONFIGURATION SETTING:
To occupy the network the mobile nodes are planned and composed dynamically. The nodes have absolute transmission extension to all other nodes according to the X, Y, Z dimensionality.

DATA ROUTING:
The sender broadcasts the data packets to destination on way intervening hop nodes using UDP user data gram protocol, link state routing like PLGP act as an ad hoc routing protocol. Sender and destination are arranged at greater distance.

INTRUSION ATTACK:
The interposed node will be violated by sending false packets if the deleterious node enters the network. So the energy of the interposed node will be exhausted by the deleterious node, the intervening energy level goes to 0 joules. The path aims to be break down between sender and destination as the data communication is violated. As a result sender redirects the data in another path to destination. The whole network will be damaged if the attack of intrusion is extended.

BACKTRACKING TECHNIQUE:

To analyse accurate nodes in the selective pathway the back tracking technique is used. After the completion of back tracking technique the nodes acquire the data. The next node certifies the source uniqueness using back tracking process if sender directs the data to neighbour node. In the presence of brute nodes the data is transmitted firmly using this technique.

INTRUSION DETECTION SYSTEM

To detect the harmful nodes from the network the energy compulsion is used, the energy level for all nodes are calculated for that objective after every data recurrence process. An ordinary energy level in most of the nodes have certain limit, due to the nature of brute nodes have an abnormal energy level like harmful node energy level is three times greater than the ordinary energy level, the malicious nodes can be identified easily by this method.

MALICIOUS NODE ELIMINATION:

The malicious nodes are encountered after the IDS process. The malicious node from the network is eliminated when the trusted authority TA instructs or warns to all nodes in the network. A secure network can be formed by exterminating malicious node.

VI. CONCLUSION

All messages have the possibility of interlope and are passed in a distributed environment in mobile adhoc network. All consensus works like to ensure whether an intrusion as taken place or not by using this messages. Cluster head and global cluster head have been provided with the secure communication in between them which will ensure the data availability, integrity, authentication and non-repudiation to be met which are security goals. More secure intrusion detection and less false positive rate can be achieved by using messages exchange processes. Hence our proposed methodology is better than the existing intrusion detection system.

REFERENCES

[1]. Sandhiya, D., K. Sangeetha, and R. S. Latha. "Adaptive ACKnowledgement technique with key exchange mechanism for MANET." In Electronics and Communication Systems (ICECS), 2014 International Conference on, pp. 1-5. IEEE, 2014.

[2]. Mohammed, Noman, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya. "Mechanism design-based secure leader election model for intrusion detection in MANET." Dependable and Secure Computing, IEEE Transactions on 8, no. 1 (2011): 89-103.

[3]. Irshad, Azeem, Wajahat Noshairwan, Muhammad Shafiq, Shahzada Khurram, Ehtsham Irshad, and Muhammad Usman. "Security Enhancement in MANET Authentication by checking the CRL Status of Servers." Int J Adv Sci Technol1 (2008): 91-98

[4]. J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, “A Framework of Combining Intrusion Detection and Continuous Authentication in Mobile Ad Hoc Networks,” 2008 IEEE Int. Conf. Commun., pp. 1515–1519, 2008.

[5]. D. Zhao, “Access control in ad hoc networks with selfish nodes,” Wirel. Commun. Mob. Comput., vol. 6, no. 6, pp. 761–772, Sep. 2006.

[6]. S. Jarecki and N. Saxena, “On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol,” IEEE Trans. Inf. Forensics Secur., vol. 5, no. 4, pp. 739–749, Dec. 2010.

[7]. S. Barker and V. Genovese, “Access Control with Privacy Enhancements: A Unified Approach,” IEEE Trans. Dependable Secur. Comput., vol. 9, no. 5, pp. 670–683, 2012.

[8]. Ghazisaidi, Navid, and Martin Maier. "Fiber-wireless (FiWi) access networks: Challenges and opportunities." Network, IEEE 25, no. 1 (2011): 36-42.

[9]. Cho, Youn Sun, and Lichun Bao. "Secure access control for location-based applications in WLAN systems." In Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on, pp. 852-857. IEEE, 2006.

[10]. Anderson, Ross. "Why cryptosystems fail." In Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 215-227. ACM, 1993.