Security to Multi-agent in IDS

[1] **G. J. Solanke,** Computer Science Department, SPCOE,Pune,India,9665166236
[2] **P. R. Chandre ,** Computer Science Department, SPCOE, Pune,India,968986310

***Abstract*— Multi-agent used to share utility to collect information from various nodes. This paper proposes intrusion detection system (IDS) which used multiple agents for accomplishing its task in mobile Ad Hoc network (MANET).The system architecture is co-operative and distributed which is divided in local intrusion detection subsystem (LIDS). Each of these LIDS participates in intrusion detection in co-operative manner for intrusion detection. But security of agent is prime issue of concern, so we are going to apply RSA algorithm on agent.**

***Index Terms*— IDS, LIDS, MANET, MAS.**

I. INTRODUCTION

Mobile Ad hoc network is wireless network where nodes shares information in unstructured network. This network is not having fixed infrastructure or topology of this network is much dynamic in nature. MANET is a network which is more vulnerable to attack, because some of the drawback explains above such as change in dynamic topology. Each node of this network is vulnerable because nodes appear, disappear or move in the network at any time, hence services provided in distributed manner in the network. Conventional approaches such as authentication and firewall for providing services could be unsuitable for MANET.

In this paper, we are going to focus on designing IDS for MANET using secure multi-agents [9]. There are two objectives of this system. First objective is to implement intrusion detection system for MANET with the help of multiple agents and second objective ensures security to the agents used in this intrusion detection mechanism. First objective can be achieved by dividing system into various local intrusion detection subsystem (LIDS). Each LIDS run in its local environment and detect the intrusion. These LIDS co-operating with their neighboring LIDS by providing them intrusion related information.

The entire task in each LIDS are accomplished by three types of agents named as detection agent, Response agent and Exchange agent. But there is more probability of attack on the data shared by the agents among each other. To secure such information , we are going to apply RSA algorithm for authenticating and encrypting information shared by the agent in each LIDS.

II. LITERATURE REVIEW

A Huge research work has been done on the IDS architecture. Researcher proposed various IDS architecture which are Categorized as standalone IDS, Hierarchical IDS, Co-operative IDS and IDS based on the agents.

Davis and Jacoboy in 2007 designed a two stage standalone IDS, in which suspicious behavior across mobile Ad hoc network can be recognized by tracking consumption of battery power of nodes in the network [4]. Results of this architecture claims 99 percentage of intrusion detection. In 2010, R.Y. Tseng and B.C. Cheng proposed context adaptive IDS for MANET. This CAIDS was based on the contextual factors such as potential security threat, residual energy and traffic loading which monitors newly arrived packets [11].

A hierarchical IDS architecture was proposed in in 2009 by two authors Chuan Xiang and Ze-Ming for clustered Ad hoc network. In this IDS, cluster head can elected through nodes which is having higher battery power[2]. Each node is made up of four modules

1. Network Detection Module: used for monitoring network packet within cluster.
2. Local Detection Module: It generate alert after identifying intruder.
3. Resource Management Module: Used for monitoring battery power of cluster head.
4. State monitoring module: This module used for check out whether network detection module is active or not.

Recently in 2011, J. Cho I. Chen ,this Chinese author also proposed scalable region based hierarchical Group Key Management Protocol with IDS architecture for facing both inside and outside attacker in MANET [10].

Architecture for co-operative IDS was proposed by Cominos and Douligeris in 2009[5]. In this architecture, three modules was created with specific task.

1. Collection Module: Used for collecting audit data.
2. Detection Module: Used for anomaly detection.
3. Alert Module: Used for raising alarm when when suspicious activity occur in the network.

Another co-operative IDS was approached by Bose S., S. Bharathimurugan and A. Kannan [1]. Study was based on multilayer intrusion detection. For example application layer, network layer, MAC etc. For local detection, each layer have its own detection engine and for global detection, three was an cross layer approach.

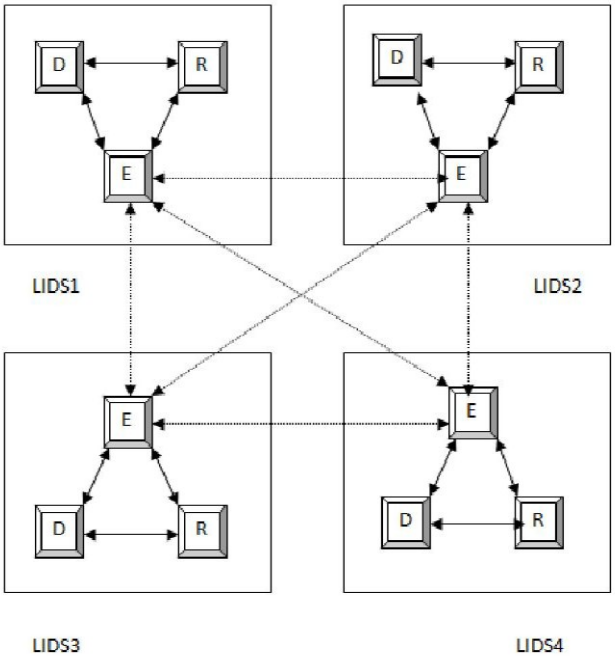
C. Ramchandra, M.S. Obaidat and S. Mishra, proposed agent based IDS for intrusion detection using FORK. FORK was two pronged strategy for detecting intrusion in Ad hoc network with the use of agents [7]. In this only those node were allowed in

ISSN: 2278 – 7798

intrusion detection process which was capable in terms of available resources. In 2008, Ramchandra et al, was come up with co-operative IDS, using light weight agents. Furthermore Farhan et al, put the idea of mobile agent based IDS, which is used for decreasing number of false positive in co-operative IDS [3]. But security of agents becomes the prime concern in agent based IDS, so it is need of advancement to provide massive security to the agents used in the IDS.

III. IMPLEMENTATION

Architecture of the system is organized in fig.1. The system actually split into different local intrusion detection subsystem(LIDS) and distributed among network [8]. Every LIDS co-operatively participate in the process of intrusion detection, each one is busy in finding out intrusion from its local traces. All of the LIDS communicate with each other for sharing attack related information or if needed get the required information from their neighboring nodes.



D-Detection Agent R- Response Agent E-Exchange Agent

Fig.1:Multi-agent based Intrusion Detection System

All these LIDS exchanges information among each other through agents. Each LIDS divided in three types of agents

1. Detection Agent
2. Response Agent
3. Exchange Agent

Every agent have some task to be done. Working mechanism of agents shown in fig.2.

Overview of Agents

A. Detection Agent:

This is one of the most essential agent of the system. Process of detection agent start by collecting data from KDD cup 99 dataset. This dataset need to be export in SQL form, it is done by SQLdumper and Wamp server. K-means machine learning algorithm applied to this dataset for the purpose of intrusion detection. This algorithm verifies that whether record of given input contains the traces of attack or it is normal data. This algorithm identifies the attack, if attack is identified as normal put records into normal cluster, otherwise place it into attack cluster, in this way k-means algorithm differentiate attack based on clustering. This clustering process can also include port scanning, if port is trusted put it into normal cluster, otherwise in the attack cluster. Next step is to determine whether the attack is known or unknown, if size of cluster with intrusion is more than maximum cluster size then it may be known as unknown attack, otherwise it is known.

ISSN: 2278 – 7798

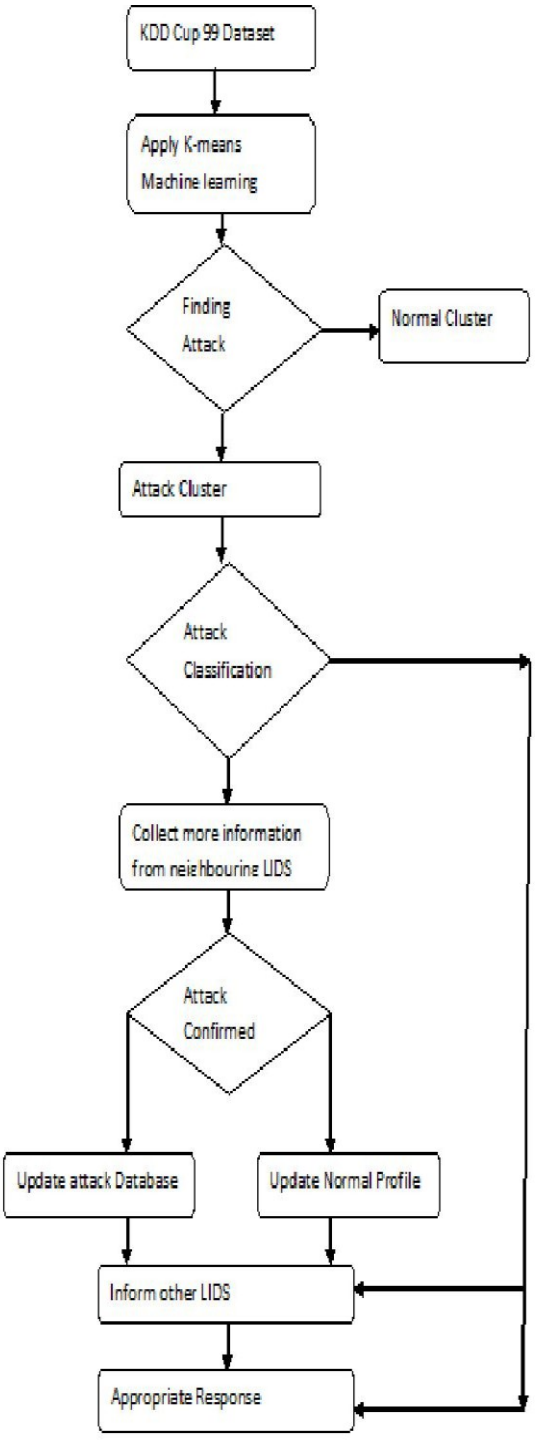


Fig.2: Detection Process

Unknown attack can be confirmed by their neighboring LIDS, IP of such a LIDS node in the MANET is put into the blacklist and informed to other LIDS nodes in the network, so that if such attacker node exist again, could be blacklisted by all other nodes in the network. After confirming unknown attack , agent transfer this information to all other nodes and updates its attack database and provide appropriate response, otherwise update database with normal profile.

B. Response Agent

This agent quickly responds to the suspicious activity in the Mobile Ad hoc network. Response agent mainly responsible for following tasks

1. Blacklisting IP of attacker node.
2. Dropping connection with attacker.
3. Updating normal profile.
4. Updating attack database.

Response agent mainly react to the port scan attack, Eavesdropping attack, data modification attack, IP spoofing attack, password injection attack, man in middle attack, compro-key attack and sniffer attack etc. which are categorized into following four types of attack

1. DOS (Denial of Services) attack.
2. U2R (User to Root) attack.
3. R2U(Remote to User) attack.
4. Probing attack.

This agent also provide magnitude of attack by dividing cluster size of intrusion detected through maximum intrusion.

B. Exchange Agent

This is the last and most essential agent in IDS which is responsible for exchanging intrusion related data among LIDS. It inform to each of the agents in every LIDS about suspicious activity in the network and also takes the additional information from them if needed. This is the only agent which communicate to detection and response agent of each LIDS in the distributed network. As this agent carries the intrusion related information between detection and response agent, so it priority to secure this agent. For this purpose, we apply RSA(Revest, Shamir, Adleman) algorithm at exchange agent to secure all this carrying information.

RSA is asymmetric cryptographic algorithm and most popular cryptographic algorithm, because it provide both encryption and authentication. It is having two keys, public and private keys. Public key known to everyone and used for message encryption and along with signature verification. Private key know only to recipient and used in decryption of messages along with creating signature.

IV. RESULT AND DISCUSSIONS

This multi-agent based architecture for intrusion detection is going to use KDD (Knowledge Discovery and Data Mining Tools) cup 99 as a input dataset, Dataset is having 86 lacs of records inclusive training and testing dataset. Each of the record is having 41 features containing discrete or continuous values. IDS faces varieties of attacks within KDD dataset, such as Neptune attack, Eavesdropping attack, Land attack, IP Spoofing attack password guess attack and sniffer attack and much more. System collects blacklisted IP and provide to every nodes in the network along with both misuse and anomaly type of intrusion detection. Rule based system provides magnitude of attack by analyzing free space on the server. System solves

ISSN: 2278 – 7798

prime issue of concern i.e. agent security with the use of RSA asymmetric cryptographic algorithm.

V. CONCLUSION

Purpose of this paper is to understand the problem in intrusion detection n MANET and build up an Multi-agent based Intrusion Detection System by considering their restriction. For such a Ad hoc network, suggested system mainly focused on security of the agents which are used in the process of intrusion detection, so that agents becomes capable for exchanging messages among them more securely with good rate of accuracy in intrusion detection.

ACKNOLEDGEMENT

I would like to express my sincere gratitude to Prof. P. R. Chandre, Head of Department and ME co-ordinator of computer science and engineering department in sharadchandra Pawar College of Engineering, Otur, Pune for the immense support and guidance for successful completion of the work.

REFERENCES

[1] Bose, S., S. Bharathimurugan and A. Kannan, ".Multi-layer integrated anomaly intrusion detection system for mobile ad hoc networks, "Proceedings of the International Conference on Signal Processing," Communications and Networking, Feb. 22-24, IEEE Xplore Press, Chennai, pp: 360-365. DOI: 10.1109/ICSCN.2007.350763, 2007

[2] Chuan-Xiang, M. and F. Ze-Ming, "A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks." Proceedings of the 2nd International Symposium on Intelligent Information Technology
and Security Informatics, Jan. 23-25, IEEE Xplore Press, Moscow, pp: 198-201. DOI: 10.1109/IITSI.2009.54, 2009

[3] Farhan, A.F., D. Zulkhairi and M.T. Hatim, "Mobile agent intrusion detection system for Mobile Ad Hoc Networks: A non-overlapping zone approach," Proceedings of the 4th IEEE/IFIP International Conference on Internet, Sept. 23-25,
IEEE Xplore Press, Tashkent, pp: 1-5. DOI:10.1109/CANET.2008.4655310, 2008

[4] Jacoby, G.A. and N.J. Davis, "Mobile host-based intrusion detection and attack identification," IEEE Wireless Communication,14: 53-60. DOI:10.1109/MWC.2007.4300984, 2007

[5] Kominos, N. and C. Douligeris, "LIDF: Layered intrusion detection framework for ad-hoc networks. Ad Hoc Network," 7: 171-182. DOI: 10.1016/j.adhoc.2008.01.001, 2009.

[6] Nadkarni K. and A. Mishra, "A novel intrusion detection approach for wireless ad hoc networks," Proceedings of the IEEE Wireless Communications and Networking Conference Mar. 21-25, IEEE Xplore Press pp: 831-836. DOI: 10.1109/WCNC.2004.1311294, 2004.

[7] Ramachandran, C., S. Misra and M. Obaidat, "FORK: A novel two-pronged strategy for an agent based intrusion detection scheme in ad-hoc networks," Elsevier Computer Communication, 31: 3855-3869. DOI: 10.1016/j.comcom.2008.04.012, 2008.

[8] Leila Mechtri, Fatiha Djemili Tolba, Salim Ghanemi, "Multi-Agent System for Intrusion Detection in MANET, "IEEE, 2012.

[9] Asmaa Shaker Ashoor and Prof. Sharad Gore," Importance of Intrusion Detection System (IDS),"International journal of scientific and Engineering Research, ISSN 2229-5518, Volume 2, Issue 1,January-2011.

[10] J. H. Cho and I. R. Chen, "Hierarchical group key management Performance analysis integrated with adaptive intrusion detection in MANET," P.E.2011.

[11] R.Y Tsseng, B.C. Cheng, "A Context Adaptive Intrusion Detection System for MANET (CAIDS)," Computer Communications, 2010.

Solanke G. J. has completed his BE degree in Computer Science and Engineering Department in Government College of Engineering, Aurangabad in 2009.Currently ,he is doing his Masters in Computer Science and Engineering. His research includes multi-agent system, mobile agent, intrusion detection system and MANET.

ISSN: 2278 – 7798