Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Agents to Secure MANETs

Taran Singh Bharati

Assistant Professor, Department of Computer Science, JamiaMilliaIslamia, New Delhi, India

Abstract: *Because of nature and requirements of mobile adhoc networks (MANETs), they are more effective in the situations where traditional wired networks cannot be operated on. As a result MANETs pass very important and confidential information from one part of network to another. There are many issues in them for example security, routing, connectivity coverage, mobility of nodes, power back-up etc. This paper deals in the security issues via mobile agents to make intrusion detection secure in the network.*

Keywords: *Security Attacks, Intrusion Detection System, Mobile Agents*

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) are the networks which are created by mobile nodes with no additional extra infrastructure. Here since there is no centralized authority for controlling. So all nodes have to work themselves in cooperative way. Routing has to be done by all nodes. Every node works as a router for passing packets to and from it. Like the wireless network, it is security lapses due to its vulnerabilities and open ports.

In an open space the messages may be intercepted by attackers for their interest. Attack is any unauthorized activity that compromises the system security. It is threat to confidentiality, availability, integrity of the system. There are two types of attacks. **Passive attacks**: in which attackers are only able to intercept the message, able to read and analyze the intercepted messages but they are not able to modify the contents and then retransmit the intercepted messages to the destination. A**ctive attacks** as compare to passive attacks active attacks are more dangerous because here attackers are not only able to intercept and read the messages but they are capable to modify the intercepted messages.

Intrusion Detection System: We have Host Based IDS that is installed in particular host machine and it will be checking for the intrusions up to host level for intrusions. If it suspects the intrusion, it reports to the system administrator so that timely remedial action can be taken.

Intrusion detection system has three parts. Data collection unit which collects the data about the activities performed by the user. Detection Engine which checks for the intrusions into the network by applying its intrusion detection methods. And last component is Communication Unit which sends alert messages to all nodes alerting them for the suspicious activities.

There are different types of IDS's like Anomaly based, Rule based and Statistical based intrusion detection. The IDS has three components Local data collection component: that collects local data about the behavior the user on the basis of activities performed by the user in his session. In order to detect whether the activity that is performed by the user is detection or not, we use misbehavior based, rule based and statistical methods on some parameters. Global data collection Component: It collects global data from all nodes in the network, and then it applies the algorithm to become assure whether not there is an intrusion into the network.

INTRUSION DETECTIONS AND THEIR CHALLENGES OF THE MANETS: As a first defense, intrusions are prevented through the encryption and decryption. But they alone are not enough. Because there are some other vulnerabilities also like, buffer overflow, denial of services, and distributed denial of services. Intrusions are detected and they are of types like anomaly based or misbehavior based.

A. ***PROBLEMS OF THE CURRENT IDS TECHNIQUES: MANETs have no such infrastructures like the fixed networks; they use only the information in communication with the nodes in their radio range and run the algorithm to detect the intrusion in cooperative manner. There are following concerns of IDS for MANETs:***
   i) **Good Architecture:** Which suites to the features of the MANETs.
   ii) **Audit Data Source**: To detect anomaly on the basis of partial, local audit traces in reliable audit sources.
   iii) **Good Activities Model:** In attacks, these can separate anomaly from the normal operations.

B. ***SOME REQUIREMENTS: The proposed IDS must have the following requirements [16]:***
   i) No new weakness should be added into the existing system
   ii) It should not consume much system resources.
   iii) Should work continuously and transparently without degrading the system performance.
   iv) It should be cooperative and open.
   v) It should minimize the false positive rate and detection must be reliable enough.

Some of the intrusion detection types are given below [14]:

i) **Signature Based Intrusions**: For detecting the intrusion into the system these IDS checks for the signature(s special pattern).If that particular types of signature is found, then an intrusion is reported. It has the drawback that

it can detect only those intrusions that keep particular types of signature. Any other intrusion that has no signature cannot be detected by it.

ii) **Statistical Based:** Statistical parameters are used to define the threshold for the detection. User behavior below the defined threshold is assumed normal and beyond the threshold behavior is treated as abnormal behavior of the user. Abnormal behavior is suspicious for the intrusions into the system

iii) **Agents Based Intrusions:** These are software programs which can and work as a spy and can get themselves installed on other machine, can collect and send their collected information about the intrusions to their masters.

iv) **Game Theoretical Based Intrusions:** Game theoretical approaches are used to model and detect the intrusions into the system, genetic algorithms, instance based learning, and neural networks can be used to detect the intrusions attacks.

v) **Data Mining and Machine Learning Based Intrusions**: Data mining and machine learning techniques like association, classification, clustering etc.

vi) **State Transition Analysis Based Intrusions**: System's or user's behavior is modeled as a state transitions diagram which has some nodes which are also called states, and edges. State is the position of the machine (CPU, memory, registers, flags, fraction of computation, etc.) at particular time of the machines. Machines rests on some state after performing its tasks it can go to another state. Machine has following components [15]:

(Q, Σ, δ, q, F)

Q: Set of all States, Σ: Set of alphabet, δ: Transition Function, q: Initial State, F: Final or Accepting States

C. *SECURITY OF THE MANETS: Following are the aspects to improve the MANETs security:*

i) **Routing Security:** To secure the route to pass the message and identification and removal of malicious (misbehaving) node from the route and transfer the information about the malicious node on the path to other nodes.

ii) **Data Forwarding Security**: When confidential data moves it should not processed by the unauthorized eavesdroppers. Data is made secure by encrypting it before sending.

iii) **Intrusion Detection Systems (IDSs):** They are the specialized tools to detect and announce the intrusions into the system.

iv) **Key Management Techniques**: In secure transmission data is encrypted by several keys. These keys are small codes which are used in various operations like encryption, decryption, message digest, and signatures. So how the keys are generated, transmitted, updated, and stored is important. In key distribution, there are two phases; first is Pre Distributed Keys and second is Post Distributed Keys.

II. MOBILE AGENTS BASED IDSs FOR MANETs

Mobile agents are the software programs. They can be moved from one machine to another, can install on machine, and can collect information about the activities of local machine and then these mobile agents send their spy information to their master, generally a manager. They are independent to the platform and architecture. Intrusion detection in mobile adhoc network is proposed in [1]. There is a local intrusion detection system (LIDS) that has many agents for various tasks like collecting of information about local activities from the management of information base (MIB) which is the source local audit trial.

These LIDS agents can be worked to collect the misuse or anomaly detection to ensure as the intrusion detection mechanism. After ensuring the intrusion into the network it is the responsibility of the LIDS to send this intrusion information to all the nodes in the network. Agents use the SNMP data which is located in MIB. SNMP takes negligible cost to collect audit data and analyze it. Agents can work in any environment because they use intrusion detection message exchange format (IDMEF) and intrusion detection exchange protocol (IDXP).

A. *AGENTS ADVANTAGES: Agents are autonomous with the following advantages [2]:*

- **Scalability**: Because of hierarchical nature different layers are established which can work either as a NIDS or a HIDS.
- **Resilience to Failure**: Failure one agent does not affect the working of the whole system. Only the tasks which are supposed to use the results of the failed agents, are supposed be down.
- **Independent**: They can work in isolation also.
- **Reduction of Network Traffic**: Agents move only important data and results t their master and hence traffic is controlled.
- **Unnecessary Restarting**: There is no need to restart the IDS, agents can added or eliminated without restarting of the IDS.
- **Solution to the Complex Tasks**: Group of agents solves the large complex tasks by exchanging their information.

B. *AGENTS CLASSIFICATION*

Agents' classification as suggested in [3,13] is as follows:

- ✓ **Reactive Agent:** they can act and transfer the information about the environment.
- ✓ **Autonomous Agents**: They are more sophisticated and can make better decision on its own tasks.
- ✓ **Temporally Continuous Agents**: They are the continuous persistent running process.
- ✓ **Commutative Agents**: They are capable enough to communicate with other nodes.
- ✓ **Cooperative Agents:** They can work together with other nodes for an intrusion detection task.
- ✓ **Adaptive Agents**: They are self-updatable and learn themselves.
- ✓ **Mobile Agents**: They can move from one node to another in the network.

C. IMPLEMENTATION OF MOBILE AGENTS

Aglets Software Kit (ASDK) and API Java Aglet (J-AAPI) are used to implement. The aglets platform executes the agents. There is an API for agents function to implement them. The language which is used here is called agent-based unified modeling language (AUML) for modeling of the system. This uses a signature based misbehave detection.

D. ARCHITECTURES

There are varieties of architectures.

i) For signature based misbehaving detection may have the following components:
   a) **Administrator Agent**: This is fixed and gathers information from all other agents about the activities decides about the intrusions and sends alert messages to all other nodes.
   b) **Crisis Agent**: To decide the minimum crisis service. If administrator agent fails, then this crisis is raised.
   c) **Analyzer Agent:** It is mobile an entity and analyses for the intrusions into the network based on the knowledge base. If it finds intrusion, it sends alert messages.
   d) **Connection Agent**: It automatically comes into picture when a session is opened for the connection.
   e) **Scan Class**: Responsible for pattern matching for intrusions.
   f) Administrator class: to manage all users in the system.
   g) **Journal of Audit**: All operations are recorded into the audit trail for later analysis.
   h) **Database Module:** That allows us to access the database of the administrator to analyze the pattern matching operations.

ii) **Layered Architecture:** Agents at different layers are proposed in [4]Following four layers of architecture are defined and each layer has some specific functions or tasks to be performed by agents which are specialized to work in that particular layer.

   a) Layer-4: Reactive agents:
   b) Layer-3: Notification agents
   c) Layer-2: Decision making agents
   d) Layer-1: Surveillance agents

iii) **Distributed Architecture using Mobile Agents:** Basically there three types of mobile agents:

   a) **Monitoring Agents**: They monitor the activities of the user.
   b) **Host Monitoring**: Every node at host level and application level is monitored.
   c) **Decision Making Agents**: This decides on the basis of threat level whether node is compromised or not.
   d) **Action Agents**: All nodes have this module to resolve the scenario of the intrusion on host.

iv) **Architecture of agents using water marking and fingerprinting:** The architecture of the autonomous agents keeps the following modules [2]:

   a) **Monitors**: They check the suspicious activities and raise the alarm on suspension into the network
   b) **Transceivers**: They are controllers of the all agents.
   c) **Agents**: They can generate the report for the attacks and send it to masters.
   d) **Filters**: they select data as per the choice.

E. COMPONENTS OF THE MOBILE AGENTS

Mobile agent must have the following components:

i) **Network Traffic or System Audit Data:** It is the traffic flow information and audit of activities data.
ii) **Local Audit Trial:** It collects local audit for suspicious activities and for normal activities.
iii) **Local Intrusion Database (LID):** Database at local system for intrusion signatures known until now. It stores the known attack signatures only and from the network traffic analysis it finds the association rules for the new unknown attack.

iv) **Anomaly Detection Module (ADM):** They work in coordination with other ADMs of other machines to detect anomalies.
v) **Misuse Detection Module (MDM):** It detects the known signature attacks defined in the local intrusion database (LID).
vi) **Secure Communication Module:** By this, IDS agents can communicate to LID, MIB, ADM, and MDM securely.

II. **Stationary Secure Database (SSD):** Database which is consulted by the agents for the latest signature about the normal user activities in a secure manner. New association rules are generated by analyzing the user activities (misused signatures). Total efficiency of system depends on the SSD.

F. SECURITY OF AGENT BASED IDSS

The agents must be protected. Apart from this, agents have other advantages like privacy and integrity of shared information. Apart from this they also have many threats i.e. agents against platforms and platforms against agents.

1) Anomaly Based Security via Mobile Agents

Nodes into the system take part in intrusion detection. Local intrusion detection is done by seeing the local audit records for suspicious activities. Some theoretical measures i.e. entropy, conditional entropy of the information flow, and classification algorithms are considered for anomaly detection.

Classifiers are trained for some characteristics for the normal behavior of the user. The features with high information gain are selected. Following methods may be used for anomaly detection: Select the audit so that normal data becomes of low entropy; do some valid data transformation as per the selected features; calculate the classifier for training data; report the intrusion, if any after the intrusion detection.

The anomaly based systems have the following components [6]:

i) **Home Agent**: This is installed in all systems and before transmitting data it confirms from its neighbors using mobile agents to know for any attack. It can be understood as:

a) **Current Node:** Home agent is installed here and it collects the information. On receiving any packet from attacker, it uses the classifier to find out the attack.
b) **Neighboring Node:** They are used to transfer the information to other systems.
c) **Data Collection:** It includes anomaly detection sub system to gather the features of the different layers.
d) **Data Pre-Processing:** Collected audit data is smoothened so as to be used in anomaly detection. Unwanted, unstructured, and irrelevant data is removed into a form which is suitable to be processed.

ii) **Cross Feature Analysis for Classifier Sub Model Construction:** Feature or character vector in the training data set, calculates the classifier. The classifier is learned from the training set by Bayesian classification algorithm with probability P. Average probability is calculated for each feature. A decision threshold is fixed. Here we can calculate the percentage of anomaly detection by the following formula:

$$\text{Percentage} = \frac{\text{Number of predicted abnormal class}}{\text{Total number of Traces}} \times 100$$

a) **Local Integration:** This ensures only the local anomaly detection.
b) **Global Integration**: This finds out the attack on the basis of overall information from total network.

iii) There three types of detection in Network based anomaly detection methods [7]:

a) **Misuse Based Detection**: They find the known patterns. They good for known attacks.
b) **Anomaly Based Detection**: They find the unusual patterns of the activities of the users. They are good for both known and unknown attacks both.
c) **Hybrid Detection:** This is themixed technique.

Anomaly types of intrusion detections are of basically two types:

a) **Performance Based Anomalies**: for example broadcast storms, congestion, paging across the network, and file servers failure.
b) **Security Based Anomalies**: they are caused by the malicious activities of the users to capture the system resources. These are of the:

i) Point
ii) Contextual
iii) Collective anomalies

Network anomaly detection is actually a classification or clustering problem which has the three components:

i) **Input Data Types**: It is a collection instance i.e. objects, records, points, vectors, patterns, events, case, observations, entities etc. the attributes may be of single valued or multi valued.
ii) **Proximity Measures Approximations**: Distance and divergence is used to check the similarity or dissimilarity between or among the patterns.
iii) **Labeling of Data**: It is done for both normal and abnormal activities.
iv) **Classification Techniques**: They are supervised, unsupervised, and semi-supervised.
v) **Feature Identification**: They are used to select the useful patterns and to remove the irrelevant patterns of the activities of the usage. The feature selections have three stages:

- **Subset Generation**: Complete, heuristic, and random
- **Subset Evaluation**: Score-based, entropy based, correlation-based, consistency-based, and detection accuracy-based.
- **Validation:** Through simulation and mathematically

2) HIERARCHICAL DISTRIBUTED SYSTEM

The network is divided into the groups or clusters [8]. Local group has local heads and it is responsible for detecting local intrusions and there is a global head responsible for global intrusion detection. There are two types of nodes, nodes with limited capabilities and the nodes with extended capabilities and coordinating capabilities. Nodes with limited capabilities can send their data to other nodes through cluster head which in turn applies the SVM to detect the intrusion into the system. This cluster has also coordinates into the global intrusion detection. Final decision about the intrusion is taken on the basis of cooperation like majority protocol, polling etc.

Fully Distributed System: All nodes into the system participate into the intrusion detection and then they broadcast their detection result into network. Nodes here detect local as well as global intrusions into the network. Architecture has the following modules:

i) **Data Collecting Module**: This generates the audit data from different network sources or nodes. It then passes this information to the SVM based detection module for analysis.
ii) **SVM-Based Intrusion Detection Module**: New machine learning technique SVM is applied to detect the intrusion.
iii) **Local Response Module**: To collect event data from the local machine.
iv) **Global Response Module**: To report the global intrusion detection into the system.

3) MANAGER BASED INTRUSION DETECTION

They are as follows:

Mobile agent is [9] installed at every host to monitor the local activities. Host controls all agents because multiple agents can be installed and run on the host involving in different activities. Agents need to be start and stop by the host.

Transceivers are devices to handle operations like controlling and processing of data. They need to be installed on every host. Every host is controlled and monitored by the system and it is called Autonomous Agents for intrusion Detection system (AAFIDS). This is the main component of the system it keeps track of the agents running on host and controls every entity. It receives report from agents and finally determines for abnormal activity into the system. Final concluded information is float to all the nodes into the system. Monitor is also a controlling module. But it is global whereas transceiver is a local controller of the host. By using agents IDS system will become more proficient in terms of scalability, difficulty in configurability, and analysis.

In Manager based [10] nodes are of two types one; ordinary types they are the local systems collect event information. While second node is a manager node which is the overall controller. Which node in the network will be the manager node is chosen by the manager selection algorithm. It has following modules:Initializationfunction,Incapablefunction,Link error function,Manager update function,Regular node update function

Performance is measured by Data Collecting Time, Expected Value E Detection Time, and Maximum Value M of Detection Time. Security issues and SVM are discussed in [11].

4) COOPERATIVE INTRUSION DETECTION IN MANETS

General requirements are suggested in [12] i.e. address the broad spectrum of attacks, intrusion detection coverage to all traffic, layered defense support, broad spectrum of detection techniques, access to intrusion data, reducing the bandwidth, and intrusion detection autonomy. Hierarchy of nodes is built by using the attributes clustering. There are some responsibilities which are supposed to be done by the nodes, are as follows:

i) **Leaf Nodes Responsibilities:** They are used for data taking, detection of intrusion and reporting some functions like:
   a) **Link-Layer Duties**: - Link layer counts and statistics of source and destination nodes are determined.
   b) **MANET Infrastructure Duties**: - Copy of infrastructure of each packet is forwarded to the cluster head time to time.
   c) **Network and Higher-Layer Duties**: - Networks also count the higher layer counts for each received packet.
ii) **Duties of the Cluster Head Nodes**: Collecting and merging its own data of intrusions from the link, network infrastructure, and higher layers detection report from its members. It applies the intrusion detection algorithm and then sends the alert messages to all nodes into its own clusters and to the cluster heads of the other clusters. Architecture has some logical parts as:
   a) **Data Source**: It is the main source of data for intrusion detection.
   b) **Dynamically Loadable Components:** Monitor for creating an input events and response modules for particular operating scenario and correlate module to combine together similar events or links.
   c) **Storage Facilities:** For local and remote events to record.

A. Identification of nodes which deliberately drop the packets.
B. Detecting the attacks on the routing in MANET protocols.
C. Attacks are detected at network or higher layer protocol

- ✓ Buffer overflow attacks inspired by HTTP, FTP, SSH, and other protocols.
- ✓ Port scans, address sweeps, fingerprinting and smart services.
- ✓ Try to gain then access of system.
- ✓ DoS and flooding attacks to congest network.

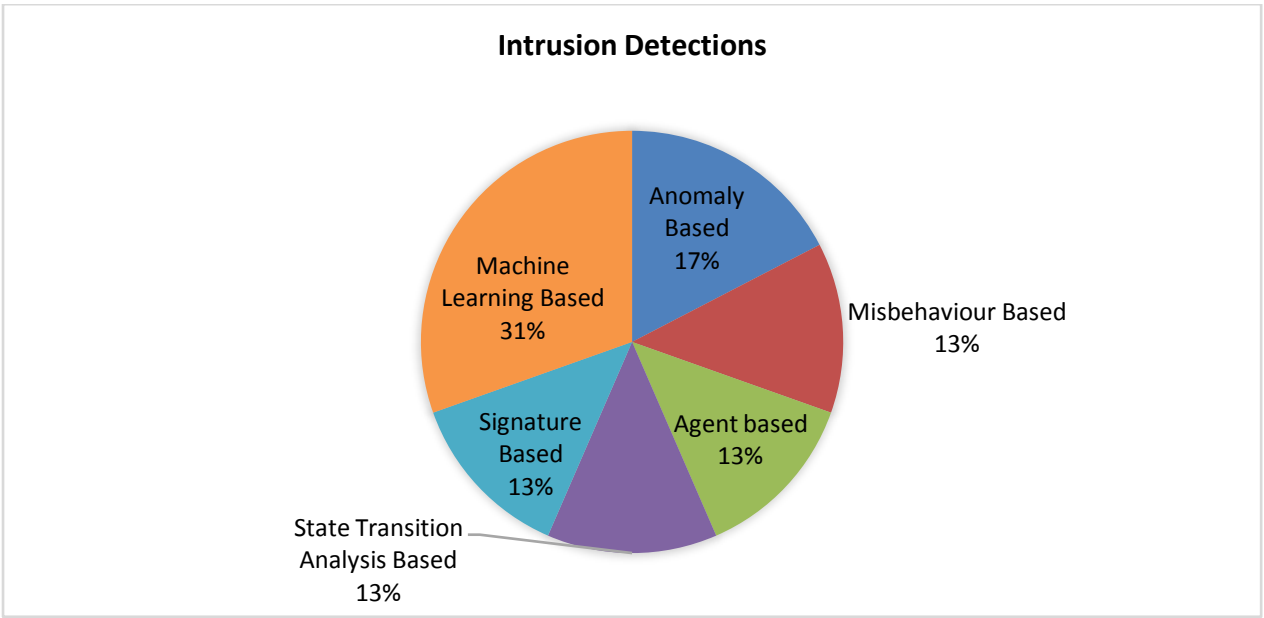
III. CONCLUSIONS AND DISCUSSION

Mobile adhoc networks are made more secure by using the mobile agents which are one of the ways to enhance the security of MANETs. This paper shows a thorough study that how agents operate, hide themselves, prevents from attackers and do the work for their master. What are the mechanisms to install, collect and send the collected secret information in a secure manner without letting someone guess that there are mobile spy code (agents) are available and doing their job. Various methods and their percentages of usage are given in table 2. Which of the parameters are or taken care of in which of the papers is also analyzed and can be seen in table 1.

Table 1: Analysis of IDSs on the basis of various parameters:

Type/Basis	Papers
Almost all parameters (A Survey paper)	Ananatvalee, T., et al., 2007]]
Misbehaviour, Collaboration, Security, Authentication	[Djenouri, D., et al.,2005]
Data Confidentiality	[Lou, W., et al,2004], [Djenouri, D., et al.,2005], [Bharati, Taran Singh, et.al., 2015]
Multi-Agents And Dempster Theory	[Wei, Z., et al, 2014], [Aljnidi, M., et al.,2007], [Bharati, Taran Singh, et.al., 2015]
Zone Based Intrusion Detection	[Sun, B.,,2003]
Cryptographic Cyclic Group, Collaborative	[Nam, J., et al., 2008]
CA, Security, Trust, Privacy, Key Management	[Zhou, L., et al,1999], [Theodorakopoulos, G.,et al,2006], [Savola, R.,2009], [Govindan, K., et al.,2012],[Savola, R. M.,2009], [Čapkun, S., et al.,2003],[Kong, J.,et al,2001], [Papadimitratos, P., et al., 2003]

Table 2: Intrusion Detection Methods' Analysis



IV. REFERENCES

[1] Mishra, A., Nadkarni, K., &Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. *Wireless Communications, IEEE*, *11*(1), 48-60.

[2] Paez, R., Satizabal, C., &Forne, J. (2006, August). Cooperative itinerant agents (CIA): Security scheme for intrusion detection systems. In *Internet Surveillance and Protection, 2006. ICISP'06. International Conference on*(pp. 26-26). IEEE.

[3] Boughaci, D., Ider, K., &Yahiaoui, S. (2007, May). Design and implementation of a misused intrusion detection system using autonomous and mobile agents. In *Proceedings of the 2007 Euro American conference on Telematics and information systems* (p. 12). ACM.

[4] Bernardes, M. C., & Moreira, E. D. S. (2000). Implementation of an intrusion detection system based on mobile agents. In *Software Engineering for Parallel and Distributed Systems, 2000. Proceedings. International Symposium on* (pp. 158-164). IEEE.

[5] Hua Zhou, Junlin Li, Na Zhao, Fei Dai, Rong Jiang, "An intrusion detection system model for adhoc networks based on the Adjacet Agent, pp. 598-601, International conference on multimedia and information technology, 2008.

[6] Esfandi, Abolfazl. "Efficient anomaly intrusion detection system in adhoc networks by mobile agents." In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 7, pp. 73-77. IEEE, 2010.

[7] Bhuyan, M. H., Bhattacharyya, D. K., &Kalita, J. K. (2014). Network anomaly detection: methods, systems and tools. *Communications Surveys & Tutorials, IEEE*, *16*(1), 303-336.

[8] Hua Zhou, Junlin Li, Na Zhao, Fei Dai, Rong Jiang, "An intrusion detection system model for adhoc networks based on the Adjacet Agent, pp. 598-601, International conference on multimedia and information technology, 2008.

[9] Muhammad ArifinRitonga and Masaya Nakayama, "manager-based architeicture in adhoc network intrusion detection system for fast detection time", international symposium on applications and the internet, 2008.

[10] Honmeideng,Quin-An Zeng and Dharma P. Agrawla, " SVM-based Intrusion detection system for wireless adhoc networks ", IEEE,2003.

[11] D.Sterne. P. Balagusubramanyam,D. Carman, B. Wilson,R. Talpade,CKo, R. Balupari et al., " A general cooperative intusion detection architecture for MANETs", Proceedings of the Third IEEE International Workshop on information Assurance(IWIA'05), 2005.

[12] KoralIligun, Recard A. Kemmere,"State Transition Analysis: A Rule-Based Intrusion Detection Approach", IEEE Transactions on Software Engineering, Vol. XX, No. Y, Month 1995.

[13] Bharati, T. S. (2015). Enhanced Intrusion Detection System for Mobile Adhoc Networks using Mobile Agents with no Manager. *International Journal of Computer Applications*, *111*(10).

[14] Bharati, T. S., & Kumar, R. (2015, March). Secure intrusion detection system for mobile adhoc networks. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on* (pp. 1257-1261). IEEE.

[15] Bharati, T. S., & Kumar, R. (2015). Intrusion Detection System for MANET using Machine Learning and State Transition Analysis. *International Journal of Computer Engineering & Technology (IJCET)*, *6*(12), 1-8.

[16] Bharati, T. S., & Kumar, R. (2016). Enhanced Key Distribution for Mobile Adhoc Networks. *International Journal of Engineering Science*, *4184*.

