Vulnerability Analysis of Mobile Agents Praxis in Mobile Ad-Hoc Networks

Bindiya Bhatia
Department of Computer Science & Engineering
Faculty of Engineering & Technology
Manav Rachna International University
Faridabad, 121001, India

M. K. Soni, PhD
Department of Electronics & Communication Engineering
Faculty of Engineering & Technology
Manav Rachna International University
Faridabad, 121001, India

Parul Tomar, PhD
Department of Computer Science& Engineering
YMCA University of Science& Technology
Faridabad, 121006, India

ABSTRACT
In the emerging world, in a resource constrained network like mobile ad hoc network, the mobile agent is becoming a favorable option for creating applications like service discovery, network discovery, automatic network reconfiguration etc. due to its astonishing features like autonomy and mobility. The joint venture of the two technologies mobile agent and mobile ad hoc network is contributing towards an ameliorate communication. There are diverse issues that are associated with mobile ad-hoc networks like the unexpected change in topology, mobility, power constraint, bandwidth limitation etc. A mobile agent is one of the solutions to conquer these challenges. A mobile agent interacts with the node in a better way and provides enhanced options for the developers to design applications based on the disconnected network. Although mobile agents take advantages over the general client-server applications, still, the mobile agents are at high-security risks due to its mobility and autonomy. The various security solutions are there to secure the mobile agents. But not all the security solutions precisely work in the mobile ad-hoc network because the network is unpredictable and subject to dynamic change in topology. The paper intends to review the vulnerabilities associated with mobile agents when applied in the mobile ad-hoc networks and studies the various approaches to overcome the risks associated with mobile agents.

General Terms
Security, Mobile agents, Wireless Networking, Analysis

Keywords
Mobile ad-hoc networks, mobile agents, security, trust based techniques, cryptography.

1. INTRODUCTION
Mobile Ad-Hoc Networks are raising wireless networks, in which mobile nodes form a network on ad-hoc basis. It is a self-configuring and self-forming network. Mobile Ad-Hoc Networks bring momentous benefits in virtually any scenario in which predetermined network infrastructure is not possible such as military areas, disaster-prone areas etc. In today's world, the computing can be done on any device, such as phones, sensors, vehicles, military equipment etc. Due to this, the affinity is towards the self-configuring and infrastructure-less *mobile ad hoc networks* (MANETs) [12]. MANET is a group of mobile nodes and connected through a provisional and spontaneous network. In MANET, there is no requirement of any central administration entity. Mobile nodes can create networks at anytime, anywhere. There is no dependency on irrelevant hardware that makes the network suitable for rescue and emergency operations [22]. The nodes in the network have limited transmission range. The nodes can forward the packets through the neighboring node in a peer-to-peer communications architecture. Due to the absence of supporting infrastructure, each node act as a router for other nodes and the routes are established cooperatively. So if a node wants to forward a packet to another node which is not in the transmission range, it can do so through the neighboring node. Thus, the neighboring node can act as a router which relays the packet further.

MANET forms a multi-hop network in which packet reach a destination through multiple hops. Generally, the wireless links have lower capacity than wired ones. Moreover, mobile nodes gain power through the portable power supplies which run out over time. Thus, bandwidth and energy consumption are the major resource in MANET which needs to be optimized.

Moreover, Routing being major service of MANET is done by taking into the consideration of mobility of the nodes. Due to the mobility of the nodes, the nodes can enter and leave the network at any time. Therefore, the network topology is dynamic and it frequently changes. Due to the characteristics of mobility, the availability of the node cannot be ensured all the time. Thus, in MANET, there is no reliability on the centralized entity. The services in MANET provides a distributed, self-organizing manner and collaborative. Auto configuration is the other service of MANET which allows the node to enter the network and fast set up without the involvement of the user.

During the last decade, MANET is gaining popularity among researchers. With the fast development in wireless communication and mobile devices, MANET plays a major job in enabling contemporary and imminent communication. MANETs are advantageous to the computing world and applicable to the areas where fixed infrastructure is impractical. However, various issues are associated with the application of MANET due to its primary characteristics, such as open medium with no observable boundaries, steady variation in topology, distributed cooperation, and bandwidth and power constraints.

Extensive research has been done to conquer these challenges. Eminent researchers worked and introduced various technologies to prevail over these issues. Mobile agent is one of the technologies.

Mobile agents are the processes which can carry code, state, and data with itself from one node to another node autonomously. It can produce child agents in the network, do the processing and then merge the results and carry back the result to its owner. Mobile agents can be used gracefully in MANETs to overcome the various problems that are associated with MANET. For e.g. mobile agent can get better utilization of the bandwidth, communication latency can be reduced and so is connection time, and the network traffic. Mobile agents can process the data over the unreliable network like MANETs. It is better to transfer the agents rather than a chunk of data from node to node over the unreliable network like MANET. But the mobility of mobile agents brings the security risks with it. The mobile agents can be malicious for the host and other agents also. There are various approaches to mitigate the risks but all the approaches cannot be precisely applied in MANET. This thought gave the motivation for the vulnerabilities analysis of mobile agent's application in MANET.

In our previous research, we have discussed the role of mobile agents in every layer of MANET [38]. This paper represents the frontward shift about the vulnerabilities that are associated with mobile agents while using them in MANET and the various technologies that can be applied to overcome these risks. The next section of the paper is discussing mobile agent's praxis in the environs of MANET highlighting the distinguished researcher's contributions. Further, the third section is throwing light on the risks that are associated with mobile agents in MANET and the various approaches that can be applied to mitigate the risks, and the fourth section presents the comparison between these approaches in the context of suitability for the MANET environment. Section five concludes the paper.

2. MOBILE AGENTS PRAXIS in MANET

A mobile agent is an independent entity that can move from one host to another host autonomously. It is a novel technique for communication and computation as a part of distributed systems. It can move to different places and carry out a number of tasks on behalf of its owner. While going through different hosts, mobile agents interact with the visited hosts to complete the task. Mobile agents interact with other hosts through communication messages. The owner of the agent can monitor its mobile agent when it migrates from host to host [5].

Mobile agents are small programs that can defer its execution on one host and migrate itself to the new host. There it can again resume its execution from where they have stopped on the previous node. There are various key features of mobile agents that make it distinguishable such as mobility, intelligence, autonomous, learning, goal oriented, network awareness etc.

In mobile computing, there is a low bandwidth and a constraint of resources. If we are using client-server approach then a continuous bandwidth is required for communication. But in the case of mobile agents, the communication can be done locally without connection which leads to bandwidth reservation. Whenever a task is completed at the remote site, the connection can be reestablished and the agent can move to its owner with the results.

Whenever the mobile agent wants to gather information from the distant node, there is no requirement for transferring the multiple request and responses across the bandwidth. The mobile agent can utilize the resources of distant node efficiently with the disconnected operation. So the loss of connection during the process doesn't affect the agent

There are a number of applications in which mobile agent technology is working such as network management, service discovery, key management, e-commerce etc. A new impending application of mobile agent is in mobile computing and mobile ad hoc networks. Due to its asynchronous & autonomous behavior, the mobile agents are good for such environments.

Figure1. is describing that the mobile agents can travel across the MANET and visit the nodes autonomously.

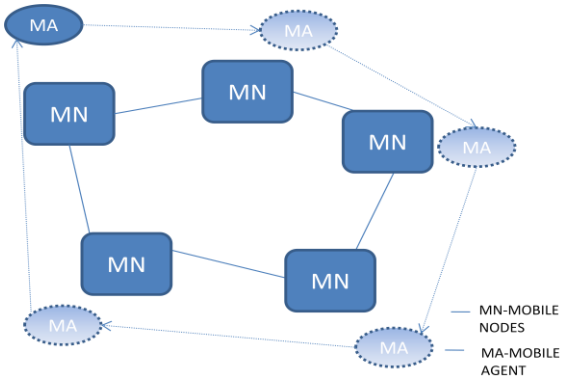

Figure 1. Mobile Agent travelling in MANET

In MANET, mobile agents can collect and process the routing information, update the topology dynamically, control the congestion, manage the key information etc.

With the practices of mobile agents in MANET, routing, congestion control, key management for security is becoming effortless and proficient. This section is discussing the work of the distinguished researchers who have applied mobile agents in the different environs of MANET.

Firstly the vital idea of using the mobile agent in MANET was taken into the sights by MIT media lab [16] with some limitations. The idea was to disseminate the routing information to the different hosts through mobile agents.

Further Chpudhury et al. [20] trailed the similar track and tried to prevail over some of the limitations of MIT's research. The authors put forward a predictive algorithm that predicts the current network topology. The mobile agents are used to collect all the topology related information and disseminate the accumulated data to the others node periodically.

Marwaha, Tham, Srinivasan [25] proposed the Ant-AODV approach which is the hybrid approach of Ad-Hoc on demand Distant Vector (AODV) and the ant based mobile agents. The authors have shown that by this technique, the end-to-end delay and route discovery latency can be reduced.

Nikos, William, Kelvin [14] applied the mobile agents and static agents to find the best path for network packets routing. The static agent runs in the background of the mobile device and continuously watches the energy of the device, capacity, and link. And mobile agents visit the nodes and gather the information collected from the static agents. The collected information is then used to find the best path.

Neogy, Chowdhury [36] designed a reliable service discovery protocol. Mobile agents are used in the protocol to accumulate service information.

Mobile agents can also be used for cluster management. Hamad, H [37] proposed the solution in which, the jobs of the cluster head is assigned to 4 different mobile agents to form the cluster, route discovery, route caching and routing. The mobile agents are residing on the member nodes and thus the load of the cluster head is deliberating on the shoulder of the mobile nodes which leads to efficient cluster management.

V. Sharma, S. Bhadauria [28] worked on control the congestion by the help of mobile agents. The intelligent and autonomous agents can read the congestion status and select the next hop for the route which is less loaded.

Similarly, the researchers are using the mobile agents for key management and security purpose. Zhang Yi, Zhu Lina and Feng Li [30] have chosen mobile agents to exchange the private key. The technique eliminates the centralized certification authority for public key distribution.

M. Darji, B.Trivedi [34] introduced the intrusion detection in MANET based on mobile agents. In this algorithm, a leader is elected based on the resource information which is collected from all the cluster nodes by mobile agents. The authors showed that it minimizes the power consumption and bandwidth.

Bindhu R [35] defined a Multi-Constrained QoS Routing Algorithm. The algorithm considered two QoS factor power and bandwidth. The authors proved in their research that, utilization of mobile agents could reduce the network delay and overhead of control messages.

Although Mobile Agents are advantageous in many environs of MANET, still the agents are reluctant to security due to their mobility. There are various security risks that are associated with mobile agents. Providing security to the mobile agents is a challenging task. The next section throws light on the vulnerabilities that are associated with the mobile agent in context with MANET.

3. VULNERABILITIES ASSOCIATED WITH MOBILE AGENTS PRAXIS IN MANETs

With the extensive praxis of the mobile agent in MANET, its security is becoming an important aspect of research. Mobile agents are vulnerable as various security threats are associated with mobile agents. Mobile agent's security risks can be classified into three major classes:

3.1 Vulnerabilities in the Interaction of One Mobile Agent to another Mobile Agent

In a multi-agent system, when a mobile agent interacts with another mobile agent there can be vulnerable situations mentioned below:

- Modification of Data or Code: Agent's code or data can be modified by another malevolent agent and thus the agent's behavior can be changed.
- Denial of Service: A malevolent agent can cause resource constraints by frequently sending messages to the other agents. Owning to this, a superfluous load is laid on the message handling routines of the receiving agent. And thus it will not be able to complete the task properly.
- Masquerade: In these types of attacks an agent pretending as host, could mislead other agents and it harms both the agent that is being deceived and the agent whose identity has been assumed, especially when agent's reputation is valued and used as a means to establish trust.

3.2 Vulnerabilities, when Mobile Agent Converse with the Node and the Node is Malevolent

Often, a mobile agent has to visit the different nodes in the network to complete a task. If any of the nodes is malevolent then vulnerable situations arise. A node that is receiving the mobile agent can simply engulf and redirect an agent and it can lead to information extraction, code or state modification, or simply ceasing it entirely. These vulnerable situations are mentioned below in detail:

- Blackhole Attack: The malevolent node spoofed the identity and pretends to be the destination node. Whenever the mobile agent reaches there, the malicious node can engulf the agent there and the agent is not forwarded further to complete a task.
- Greyhole Attack: It is a kind of selective blackhole attack in which the malevolent node act properly for some time and then behave maliciously. It drops the agent selectively so that the node can't be detected.
- Wormhole Attack: Whenever the mobile agent reaches to the malevolent node, it redirects the agent to somewhere else and the agent never reaches its destination node.

3.3 Vulnerabilities, when a Mobile Agent Converse with the Node and the Mobile Agent is Malevolent:

The malevolent mobile agent can exploit the security weaknesses of a node and harm the node. Different types of vulnerable situations can be there:

- Denial of Service: Agent utilizes an abundance amount of host resources, so that the host won't have the capacity to service other agents legitimately.
- Unauthorized access: If an agent gets the entrance to the host then unauthorized agent can damage the host.
- Masquerading: The malevolent agent pretends to be an authorized agent to gain access to services and resources to which it is not entitled.
- Energy Consumption: In MANET, mobile devices operate on battery. So, the battery power is the important resource in the network. The Malicious mobile agent can consume the power of the host by interacting unnecessary with it.

4. DEFENSE MECHANISMS

Extensive work is reported to defend against above mentioned vulnerable situations. Some of the mechanisms are proposed to protect only the mobile agent's code and some of them are to protect the host platforms. The discussion is as follows:

- Sand Boxing

R. Lakshmi, A. Vincent Kumar [19] proposed the sandboxing technique which is used to protect host platform from malicious mobile agents. On host platform, local code is executed with full permission and has access to all system resources. But the execution of the remote code, such as mobile agents and downloadable applets, is done inside a restricted area called a "sandbox".

- State Appraisal

W. M. Farmer, J. D. Guttman, and V. Swarup [29] defined State appraisal mechanism which is utilized to find any change or alteration in the state of the agent at any malignant host platform. Whenever the mobile agent reaches to the new host, it must decide the privileges that it requires at the new site. A state appraisal function is there, to determine the set of permissions to be requested to the new host. It will find the maximum set of privileges that the agent could request to the host. The sender sends the mobile agent and this state appraisal function to the destination host. Upon receiving the destination host, the host verifies the state of the mobile agent and decides after the verification process, what permissions can be granted to the agent.

- Proof-Carrying Code

G. C. Necula and P. Lee [8] proposed Proof-Carrying Code (PCC). In this technique, the code of the mobile agent is verified by the host that the code adheres to a predefined set of safety rules. The mobile agent generates the formal safety proof that the code will follow the defined safety policy. To implement PCC, the specifications are written in first order logic and the code is in the form of the machine code. Floyd's verification-condition generator is used to extract the safety properties of the machine code programs as a predicate in first order logic. The mobile agent tries to prove this predicate by axioms and inference rules supplied by the host as a part of safety policy. And then Edinburgh logical framework is used to check the proofs. The advantage of the PCC is that there is no requirement of cryptography or trusted third party. The PCC programs are self-certifying. But it is not an appropriate practical approach for complex and larger code.

- Environment Key Generation

Riordan J., B. Schneier [33] have proposed environment key generation scheme to secure the mobile agent through cryptography. In this scheme, the key for encryption was generated through certain classes of environmental data. The agent could decrypt the encrypted message only when the environmental conditions would be true. For e.g. the key could be generated by applying hash functions to a particular message of a Usenet newsgroup. A key could be placed in a file, the hash of a file or the hash of a particular file name; the key can be found in the content of a mail from the sender; or a key can be generated by applying hash to local DNS block transfer or a broadcast ping packets. There could be time stamp construction also where key generation depends on time. It can be forward time construction where the key is generated before the particular time stamp or the backward time construction where key generation is done before a particular time.

- Location Privacy through user smart card

B. Askwith, M. Merabti, Q. Shi and K. Whiteley [3] defined a technique which provides privacy to mobile agents in terms of content & location. The user in this scheme registers to the network but remain anonymous. The user is having the subscriber identity module-smart card and a terminal. The user communicates with the local networks and the external user communicates with the mix of local and home networks. The subscriber identity module carries the user's personal account details and it allows the user to be connected to the network through the terminal. The network updates the location information whenever the terminal is switched on and the user is moving from one location to another. At the time of registration, the user requests authentication with the local networks. The local network passes this information anonymously to the home network. Then a challenge is issued to the user by home networks via local networks return address. The response is sent to home network & then the home network user be allowed to reply to local network's request for mobile user authentication. The following steps explain the communication process:

i. First, mobile user requests the registration to the local networks.

ii. Then local network sends the authentication request anonymously.

iii. The home network sends a challenge to mobile user via the local network.

iv. The mobile user responds to this challenge via the local network.

v. The mobile user is authenticated now.

vi. Also, the local network sends the authentication request to the home network for its authentication.

vii. The mobile network sends token to the local network and mobile user and then the local network is authenticated.

All the communication between local and home networks use digital mix [6]. The home network doesn't know the location of the user, it is only aware of the digital mix return address that was given by the user in the registration process. Thus, the location privacy is achieved.

If an attacker tries to discover information, the attacker will only be able to find the identity of the digital mix. The location of the user would not be found by the user due to untraceability created by the mix.

- Obfuscation

This technology protects the code of the mobile agents from being analyzed by the malicious host [7]. Three core techniques are used to provide strong protection to the mobile agents:

- Distributed Agent State: The agent is divided into the set of communicating software code (agentlets). Each code executes on independent hosts.
- Obfuscation with periodic Regeneration: Variety of techniques is used to obfuscate agentlet's code and data.
- Monitoring & Recovery: Each agentlet is made self-monitoring & also the agentlet is able to monitor other agentlet.

Obfuscation transforms a program into another program whose behavior is same but the obfuscated program is much complex to understand. For this, obfuscation policy & obfuscation transformation procedure is there. Both program and obfuscation policy fed into transformation function & an obfuscated program is generated which is semantically

identical to the program but its state and behavior is obscure to any attacker who has not any knowledge about the program. Hohl [7] used the Obfuscation technique to get a time limited black box agent that can be executed safely on a malicious platform for a certain period of time but not forever.

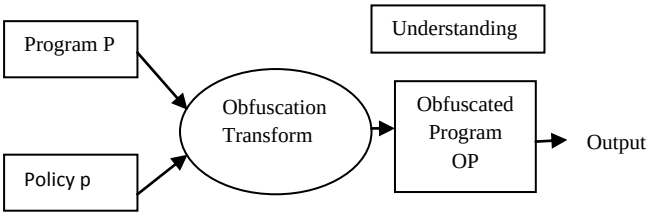

Figure 2. Obfuscation

- Secure Image Mechanism

Tarig M A. [27] introduced the technique to guard the mobile agent against malicious hosts. There is a secure image controller (SIC). Before sending the mobile agent to the host, the agent moves to SIC. The SIC send an image of the mobile agent to the host with different contents. When the image returns to SIC, it inspects the image to check against any alteration attack. If SIC found no alteration then the data for each task that is assigned to an agent to perform on a host is first digested using hash function & then has been given to the agent. Also, the agent is encrypted using one secret key except for the agent that relates to the untrusted host.

Whenever the image of an agent visits the untrusted host, the SIC wait for the image for the specified time. If it doesn't return back within the specified time, the SIC ignore the host and doesn't send the agent to that host. If it returns back then it creates the digest of the data and compares this data with the original data to detect the alteration attack. If there is a change in the data that means the image is altered.

The technique is not suitable for MANET because in the technique the SIC is the central entity and it becomes a bottleneck to the resource constrained environment of MANET.

- Trust Enhanced Symmetric Key Cryptography

In this technique [9], a trusted third party is used for key generation. A key agreement is done with trusted host via KBS (Knowledge Base System). KBS is host which maintains the information regarding trusted hosts. Whenever an agent reaches the trusted host, it appends the data that is generated on the host with the data carried by the agent. The data is then encrypted and the identity information is verified by the KBS. The algorithm is as follows:

i. Before creating the mobile agent, a key agreement is done between the host (S_0) and the KBS using Deffie – Hellman Key exchange algorithm.

ii. The host generates mobile agents for the specific task.

iii. Mobile agent migrates to the trusted host (S_i) with encrypted data. The original data can be computed through computation on trusted host.

iv. Mobile agent verifies& appends the current host data with all the previous host data.

v. After that, it migrates to next trusted host (S_{i+1}) & do the same.

vi. After passing through n hosts mobile agent returns to S_0 with collected data. Mobile agent decrypts the collected data through its private key & compute hash value by performing the hash function on decrypted data. If the hash value is same that means the data is not altered anywhere. If the data is not altered then the mobile agents pass the collected data to S_0 otherwise it sends the information that data is damaged.

- Threshold Cryptography

Sultanik et al [26] presented a technique to secure mobile agents in ad-hoc wireless networks through threshold cryptography. The authors provided a framework SWAT (Secure Wireless Agent Test bed) for information assurance of mobile agents. It incorporates cryptography and ensures the different group of agents will be able to create secure communication channels among overall agent community. Cryptography infrastructure is used by the agents to execute various assignments such as authentication, group key generation, revocation, non repudiation. In SWAT, the agents have decision power and have reasons for its own activities. SWAT uses the Extendable Mobile Agent Architecture (EMAA). EMAA provides the framework for agent mobility, events and communication between agents. It also supports Distributed Event Messaging System. AODV protocol is used for routing. Numbers of existing techniques are used in the framework such as CLIQUES is used for a key generation; SPREAD, client-server application is used for group communication; Semi-Trusted Mediator (SEM), an algorithm for user revocation and IPSEC is used for encryption and decryption of the data on the network layer.

In this technique, a master public/private key pair is there to sign a certificate. The master public key is known to all hosts and any certificate is trusted if it is signed by the master private key. Master Private Key is divided into a no. of shares and is stored in a group of nodes. Whenever the host wants to decrypt the agent, the shares of the private key should be collected to form the master private key. But it may be possible that, due to node mobility, transient failure of the links and limited battery backup, a node of the group having one share may not be available to give its share and hence the entire system performance would degrade.

Also, the technology is limited to secure inter-agent communication.

- Combination of Recognition and Protection Mechanism to protect mobile agent integrity

Haghighat, R., Yarahmadi, H [10] proposed the scheme in which three agents are used. First, the dummy agent moves to the host and returns with results of the calculations back to the original agent. If the results indicate a safe host then the agent records the path with the Record agent and then the Keep Agent encrypts its data to move to the host platform. But this system requires a lot of bandwidth which is expensive in MANET.

- Trust-based security technique

In [32] trust-based mechanism is proposed in which cooperative behavior of the agents and nodes help to secure the mobile agent. The reputation of a node can be calculated by taking the observation of the neighboring node. The trust is categorized as belief, disbelief, and uncertainty and mathematically can be expressed as

$B+d+u = 1$

The reputation of a node can be quantified by the feedback from the agents and the node. The feedback can be from direct observation (experience of mobile agents while

traveling to nodes) and indirect observations (feedback, the mobile agent collects from neighboring node about a particular node).

In the case of direct observation, the agent's experience is quantified through beta distribution (α, β). The α_{ij} parameter is for number of good transaction when agent interacts with a node & is incremented as

$$\alpha_{ij}(new) = w * \alpha_{ij}(old) + (1-w) * p_j^k$$

Where, p_j^k is the agent's observation about node j. It is weighted observation and it ranges from (0<w<1).

And $\beta_{ij}$is considered for bad transaction i.e. the agent doesn't come back to the owner.

$$B_{ij}(new) = w * \beta_{ij}(old) + (1-w) * p_j^k$$

The uncertainty of a node can be calculated as

$$U_{ij} = \frac{12 * \alpha_{ij} * \beta_{ij}}{(\alpha_{ij} + \beta_{ij})^2 + (1 + \alpha_{ij} + \beta_{ij})}$$

The node also shares the information about the malicious node with other nodes through agents. Through this indirect observation the belief on a node can be calculated as

$b_l^{i:j} = b_j^i * b_l^j$

where b_j^i is the belief of node i on node j and b_l^j is the belief of $node_j$ on $node_l$. $b_l^{i:j}$ is the belief of $node_i$ on $node_l$ while taking feedback from observation of $node_j$.

The direct and indirect result is combined to find the reputation of a node.

In this scheme, the cooperative behavior of nodes is considered to secure the mobile agents and there is no requirement for any centralized node. So the approach can be considered for MANET.

5. COMPARISON OF THE DEFENSE MECHANISMS TO SECURE MOBILE AGENTS WHILE CONSIDERING THE MANET ENVIORNMENT

As per the above discussion, it is visible that the approaches are proposed either to protect the mobile agent or the host. Very few works address the entire security aspects of mobile agent system in a mobile ad hoc network. Due to the mobility of node and resource constrained environment in MANET, some of the approaches are not well suitable to provide security to the mobile agents. Table 1 is illustrating the comparison between the approaches on the following parameters:

1. Whether the approach is suitable to secure the mobile agents in MANET environment.
2. Whether the approach is providing security to the mobile agent or the host.

Table1. Comparison of different approaches to secure mobile agents

S No.	Defense Mechanism	Suitability in MANET Environment	Security intention
1.	Sand Boxing	Suitable for MANET	Providing security to the host platform only
2.	State Appraisal	Suitable for MANET	Securing the Mobile agent's state
3.	Proof -Carrying Code	Suitable for MANET	Providing security to the host platform only
4.	Environment Key Generation	Not Suitable for MANET	Securing the mobile agent's code and data
5.	Location Privacy through user smart card	Suitable for MANET	Mobile agent's data is secured
6.	Obfuscation	Suitable for MANET	Securing only Mobile agent's code
7.	Secure Image Controller	Not Suitable for MANET due to centralized third party	Securing Mobile Agent's code and data
8.	Trusted Enhanced Symmetric Key Cryptography	Create bottleneck in MANET due to the third party.	Securing Mobile Agent & Host
9.	Threshold Cryptography	Not Suitable for resource constrained environment of MANET	Mobile Agent & Host are secured
10.	The Combination of recognition	Very expensive in	Only Mobile

	and protection mechanisms to protect mobile agent integrity.	MANET due to requirement of Bandwidth	Agent's data is secured
11.	Trust-based security Technique	Suitable for MANET	Securing mobile agent's data and host

The above table concludes that various approaches are there to secure the mobile agent, some use cryptography and the various techniques for key generation, some use trust etc. But very few of them provide the complete security solution in a resource constrained environment like MANET. They either provide the security to the mobile agent or host. But don't take contemplation of both. And only some of them are providing security to the state of the mobile agent.

6. CONCLUSION AND FUTURE SCOPE

Now a day mobile agent seems to be a popular choice to perform the various function like topology discovery, network management, congestion management, key management, routing, automatic network reconfiguration etc. for resource constrained environments like MANET. Many a time, the task processing is taken up by mobile agents that autonomously travel in the network and get the task done.

Although, mobile agents practice in MANET is suitable and efficient still, securing mobile agents is a big concern particularly when, the network usually undergoes continuous topology changes. Mobile agent security emphasizes on protecting and preventing a mobile agent from malicious hosts' attacks by applying cryptographic functions and other mechanisms. There are lots of security approaches to secure mobile agents as mentioned in section 4. Some use cryptographic functions to provide authenticity, data integrity and non repudiation. Some use the trust to prevent attacks like blackhole and wormhole. But still, lots of problems exist with the present security approaches.

There are lot of unsolved problems, challenges and issues with the existing system and few needs more improvisation. Some of the issues are mentioned below and can be considered to work upon in future:

- The existing approaches either consider the attacks by hosts or attacks by agents, but very few of the approaches had taken the consideration of providing security to the whole environment.
- Few of the existing approaches give the complete security solution.
- Mobile devices work on battery and very few of the existing approaches take battery constraint of MANET into consideration.
- Only a few technologies provide security to mobile agent state and protection of mobile code against input and output analysis.

7. REFERENCES

[1] Abdulrahman Hijazi, 2005. Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks. Wireless and Optical Communications Networks. WOCN 2005. Second IFIP International Conference on March 6 – 8. 2005.

[2] Alexandre Manguer, 2003. Mobile agents in ad hoc networks. Thesis. April 2003.

[3] B. Askwith, M. Merabti, Q. Shi and K. Whiteley. 1997. Achieving User Privacy in Mobile Networks. Proceedings of the 13th Annual Computer Security Applications Conference. San Diego. pp. 108-116.

[4] Borselius, N. Mobile agent security. 2002. The Electronics & Communication Engineering Journal. Vol 5. pp. 211–218.

[5] Prakirti Raghuvanshi et al. 2015. A Modified Agent Based AODV Routing Protocol for MANET's. (IJCSIT) International Journal of Computer Science and Information Technologies. Vol. 6 (4). 3298-3301

[6] Chaum. 1985. Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of ACM. Vol 28. No 10. pp. 1030-1044.

[7] F. Hohl. 1998. Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts. Appear in Mobile Agents and Security Book edited by Giovanni Vigna. Published by Springer Verlag.

[8] G. C. Necula, P. Lee. 1997 Research on proof-carrying code on mobile-code security. DARPA Workshop on Foundations for secure mobile code. March 26-28, 1997.

[9] G. Geetha, C. Jayakumar. 2011. Trust Enhanced Data Security in Free Roaming Mobile agents Using Symmetric Key cryptography. International Journal of Network Security & Its applications (IJNSA). Vol.3. No.5.

[10] Haghighat, R., Yarahmadi, 2008. H. A New Approach for Mobile Agent Security. In: The Proc. of the World Acadamy of Science, Engineering and Technology. vol. 32.

[11] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks Vol 1. pp. 13–64.

[12] Karlsson, Jonny,Dooley, Laurence S. and Pulkkis, Goran. 2012. Routing Security in Mobile Ad-hoc Networks. Issues in Informing Science and Information Technology. Volume 9, 2012. pp 369 – 383.

[13] L. D'Anna, B. Matt, A. Reisse, T. Van Vleck, S. Schwab, and P. LeBlanc. 2003. Self- Protecting Mobile Agents Obfuscation Report. Report #03-015. Network Associates Laboratories. June 2003.

[14] Nikos Migas, William J.Buchanan, and Kevin A. Mcartney. 2003. Mobile Agents for Routing, Topology Discovery, and Automatic Network Reconfiguration in Ad-Hoc Networks. in proceeding of 10th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03).

[15] N Kawaguchi, K Toyama, Y Inagaki. 2000. MAGNET: ad hoc network system based on mobile agents. computer communication. volume 23. issue 8. pp 705-782.

[16] N. Minar, K.H. Kramer, and P. Maes. Cooperating Mobile Agents for Dynamic Network Routing. MIT Media Lab. Link: http://xenia.media.mit.edu/~nelson/research/ routes-book chapter/minar.pdf

[17] Rajesh Shrivastava, Pooja Mehta (Gahoi). 2012. Analysis of Secure Mobile Agent System. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307. Volume-2. Issue-1.

[18] Rizvi, S.M.S.I., Sultana, Z., Bo, S., Islam, M.W. 2010. Security of Mobile Agent in Ad hoc Network using Threshold Cryptography. In: The Proc. of the International Conference on Cryptography, Coding and Information Security.

[19] R. Pushpa Lakshmi, A. Vincent Antony Kumar. 2010. Cluster Based Composite Key Management in Mobile Ad Hoc Networks. International Journal of Computer Applications (0975 – 8887). Volume 4 – No.7.

[20] R.R. Chpudhury, S. Bandyopadhyay, and K. Paul. 2000. A distributed mechanism for topology discovery in ad hoc wireless networks using mobile agents. In Proceedings of First Annual Workshop on Mobile Ad Hoc Networking Computing. MobiHOC Mobile Ad Hoc Networking and Computing. August 11, 2000

[21] R. Wahbe, S. Lucco, T. E. Anderson, and S. L. Graham. 1993. Efficient software-based fault isolation. In Proceedings of the 14th ACM Symposium on Operating Systems Principles. Pages 203—216. Dec. 1993.

[22] Saleh Ali K.Al-Omari, Putra Sumari. 2010. An overview of mobile adhoc networks for the existing protocol and applications. International journal of application of graph theory in wireless ad-hoc networks and sensor networks. Vol 2. No.1.

[23] Samuel Lee. Mobile Agents. A tutorial report. Agent based software engineering.

[24] Sathish Alampalayam Kumar. 2010. Classification and Review of Security Schemes in Mobile Computing. Wireless Sensor Network. vol 2. pp 419-440

[25] Shivanajay Marwaha, Chen Khong Tham, Dipti Srinivasan. 2002. Mobile Agents based Routing Protocol for Mobile Ad Hoc Networks. Global Telecommunications Conference, GLOBECOM '02. IEEE volume 3. pp 17-21.

[26] Sultanik, et al. 2003. Secure Mobile Agents on Ad Hoc Wireless Networks. The Fifteenth Innovative Applications of Artificial Intelligence. Conference Acapulco. Mexico.

[27] Tarig, M.A. 2009. Using secure-image mechanism to protect mobile agent against malicious host. In: Proc. of World Academy and Science, Engineering and Technology. pp. 439–444.

[28] Vishnu Kumar Sharma, Sarita Singh Bhadauria. 2012. Agent based Congestion Control Performance in Mobile ad-hoc Network: A Survey paper. (IJACSA) International Journal of Advanced Computer Science and Applications. Special Issue on Wireless & Mobile Networks.

[29] W. M. Farmer, J. D. Guttman, and V. Swarup. 1996. Security for mobile agents: Authentication and state appraisal. in Proceedings of the European Symposium on Research in Computer Security (ESORICS'96). ser. Lecture Notes in Computer Science, E. Bertino, H. Kurth, G. Martella, and E. Montolivo. Eds vol. 1146. Rome. Italy: Springer. September 1996. pp. 118–130.

[30] Zhang Yi, Zhu Lina and Feng Li. 2009. Key Management and Authentication in Ad Hoc Network based on Mobile Agent", Journal of Networks, Vol. 4, No. 6.

[31] Mats Person, 2000. Mobile Agent Architectures. Scientific Report. Dec 2000. Defence Research Establishment. ISSN 1104-9154.

[32] Chandreyee Chowdhury, Sarmistha Neogy. 2011. Securing mobile agents in manet against attacks using trust. International Journal of Network Security & Its Applications (IJNSA). Vol.3. No.6.

[33] Riordan J., B. Schneier. 1998. Environmental key generation towards clueless agents. in Mobile agents and security. Springer. p. 15-24.

[34] M. Darji, B.Trivedi. 2012. Secure Leader Election Algorithm Optimized for Power Saving. Proceedings of international conference on Recent Trends in Computer Networks and Distributed Systems Security. Trivandrum. India. October 11-12. DOI: 10.1007/978-3-642-34135-9.

[35] Bindhu.R. 2010. Mobile Agent Based Routing Protocol with Security for MANET. International Journal of Applied Engineering Research. Dindigul Volume 1. No1.

[36] Neogy, R.; Chowdhury, C.; Neogy, S. 2012. A reliable service discovery protocol using mobile agents in MANET. Reliability and Maintainability Symposium (RAMS). Proceedings – Annual. vol. no. 7. pp. 23-26. Jan, 2012. doi: 10.1109/RAMS.2012.6175451.

[37] Hamad, H. 2008. Distributed Mobile Agents for reliable cluster management in MANETs. International Journal of Interactive Mobile Technologies (iJIM). Issue 2. vol. 2. Apr. 2008. pp. 11-17.

[38] B Bhatia, M K Soni, P Tomar. 2015. Role of Mobile Agent in Layered Architecture of Mobile Ad-Hoc Networks. I. J. Computer Network and Information Security. 11, 37-45, DOI:10.5815/ijcnis.2015.11.04