Security Feature in MANETs – A Review

Nisar Ahmad Malik
MM University
Mullana
Ambala Haryana

Munishwar Rai, PhD
MM University
Mullana
Ambala Haryana

ABSTRACT

The mobile Ad-hoc Network is infrastructureless network, self-organizing on demand wireless network. It means the formed network can be deformed on the fly without any centralized control. This gives rise to topology change and in turn exposes MANETs to different security attacks. And to deal with these topology changes different protocols have be devised and discussed in this paper but still these protocols are not fully capable to cope up these challenges and are open to researchers for proper attention. A Mobile Agent has a unique feature to move from one system to another in the same network. This ability helps researchers to cope up with security issues in MANETs to some extent.

General Terms

MANETs, attacks, routing protocols, AODV, CSRP, Mobile Nodes (MA), APVP, QoS, IDS, malicious nodes, black hole

Keywords

MANETs, attacks, AODV, CSRP, Mobile Nodes (MA), APVP, QoS, IDS.

1. INTRODUCTION

Communication technology have evolved as one of the most transforming and empowering technology in recent years, particularly mobile ad hoc networks (MANETs) are the most popularly studied network communication technology[6]. The Mobile Ad-hoc network term was proposed by Internet Engineering Task Force in 2002 [1].

Mobile Ad hoc Networks are infrastructure less communication networks. Infrastructure less network means that they does not have pre-existing infrastructure [3][11] i.e. base stations and access points see Figure 1. MANETs have a decentralized network infrastructure, thus all nodes are free to move randomly. MANETs have the capability of creating self-configurable and self-maintaining network without any centralized infrastructure. The participating nodes in a MANET may be mobile phones, laptops, palm tops, PDA, sensors nodes etc. each of which is equipped with a wireless transmitter and receiver device. The node may be located anywhere in aeroplanes, ships, trucks, cars perhaps even on people or in very small devices. The radio range of any node in the network defines its neighborhood, where a node may use simple broadcast to establish a communication link with the neighboring nodes. However the radio range is declined by the interference. Due to the limited range of nodes, the nodes that are out of range need to rely on intermediate nodes, the intermediate nodes act as routers, which discover and maintain routes to other nodes. Such networks are referred as Multi-Hop or Store-and-Forward networks.

MANETs are supposed to be useful in [1][2][11][11] disaster recovery, battle field, communications and rescue operations where infra structured networks does not exists or get damaged due to some disaster. It is proved to be a feasible means for ground communication and information sharing. Due to ubiquitous computing, dynamic topology, lack of centralized infrastructure and tactical applications like battle fields and other military services MANETs give rise to many security risks that need proper attention for their deployment.

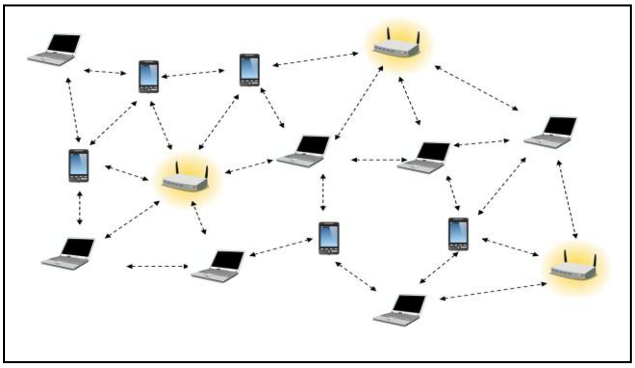

Figure 1: Mobile Ad-hoc Network (MANET)

1.1 Overview if MANETs

a) Characteristics of MANETs

In MANETs the devices having wireless and networking capabilities can communicate with each other. It gives rise to following characteristics:

- **Distributed operation:** In MANETs, each device act as both host and router i.e. every node is autonomous in behavior.
- **Dynamic topology**: The nodes can join or leave the network anytime, making the network topology dynamic in nature. Remaining nodes at any point of time can establish their own network again.
- **Light-weight terminals**: Mobile nodes are characterized with less processing speed, less memory and battery power. Sometimes these nodes are called "thin clients".
- **Autonomous Establishment**: MANETs are having mobile and spontaneous behavior which demands minimum human intervention to configure the network and can have high user density and large level of user mobility.
- **Router Free:** For connecting nodes to the network no router is needed, due to this running an ad-hoc network is more affordable than traditional network.
- **Mobility:** The nodes in Ad-hoc network can move freely in the network in any direction. Issues concerning mobility of participants are dealt by routing algorithms.
- **Speed:** Setting an Ad-hoc network from scratch requires few setting changes and no additional hardware or software is needed. If we need to connect multiple nodes in a network quickly and easily then MANET is the ideal solution.

- **Connectivity:** Because of decentralization within MANETs every node is fully collaborating in the task of delivering packets.
- **Fast Installation:** MANETs are highly flexible to install, because no base stations or access points are needed, thus they can be installed in very less time e.g. in case of natural disasters like floods or earth quakes we can install MANETs quickly, but unfortunately it was not done in recent flood in Jammu and Kashmir.
- **Cost:** MANETs could be economical in some situations as fixed infrastructure cost could be eliminated and power consumption is reduced as compared to fixed wireless networks.

b) Working of MANETs

A MANET is self-organizing and adaptive network. It means that a formed network can be deformed on-the-fly without the need for any system administration. There are no fixed routers in MANETs, each node (mobile communicating device) can act as router. Each node has the responsibility of organizing and controlling the network. The communication in MANET can be established through cooperation among the devices themselves. In simplistic realization of the communication concept a mobile device interested in communicate can forward its packets to neighbor who in turn forward it to its neighbor and so on until the destination node is reached. This forms a simple ad-hoc network. Based on this concept Figure 1.2 illustrates a schematic model of simple ad-hoc network comprising of four mobile devices viz. A, B, C and D. Suppose mobile device A wants to communicate with D. Assuming that A and D are not within the radio range of each other and cannot directly communicate with each other. However they can take help of node B and C to relay packets to each other.

There are no hard and fast rules for topology in MANETs. The MANETs topology is dynamic in nature that means the topology can change dynamically for various reasons. In MANETs topology changes as nodes move out of radio range of one or more nodes with which they were connected and move closer to connect with other nodes. In addition to this even in fixed ad-hoc networks (e.g. wireless sensor fields) due to limited bandwidth or wireless link (subjected to fading and jamming) or of the nodes themselves (e.g. damaged due to hostile condition or discharge battery) the logical topology may change.

To deal with these topology changes different protocols are there for smooth communication within MANETs, which are discussed next.

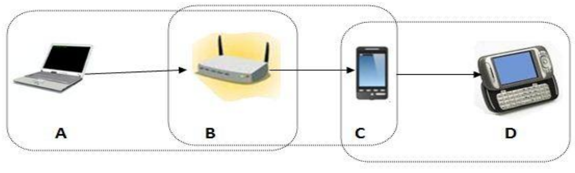

Figure. 1.2: Working of MANETs

c) Communication protocols in MANETs

Protocols are set of rules and regulations that govern the smooth communication between the communicating devices. There are three main categories of protocols: Figure. 1.3

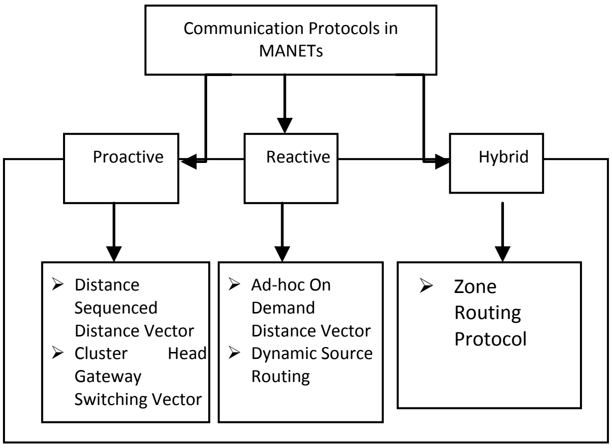
Communication Protocols in MANETs
Proactive
Reactive
Hybrid
➢ Distance Sequenced Distance Vector
➢ Cluster Head Gateway Switching Vector
➢ Ad-hoc On Demand Distance Vector
➢ Dynamic Source Routing
➢ Zone Routing Protocol

Figure 1.3: Categories of Communication Protocol

(i) Proactive

(ii) Reactive

(iii) Hybrid

(i) Proactive*:* In proactive ones the nodes maintain up-to-date routing information ahead of demand. The strategy of these protocols is to follow an optimal path. For example Destination Sequenced Distance Vector (DSDV) and Cluster Head Gateway Switching Vector (CGSR) are proactive protocols.

- **Destination Sequenced Distance Vector (DSDV):** It is one of the earliest protocols found in MANETs. The base of this protocol is distributed Bellman-Ford routing algorithm. In distance vector protocol each node maintains a routing table (e.g. in number of hops) to each destination along with the next-hop neighbor on that path. The tables are updated periodically among the neighboring nodes.
- **Cluster Head Gateway Switching Vector (CGSR):** In hierarchal networks, nodes are grouped into clusters and each cluster is headed by a special node called cluster head. These nodes belong to different clusters and act as gateways among different clusters.

(ii) Reactive*:* In Reactive protocols they collect necessary routing information only when it becomes explicitly needed to sustain an actual session. In general routing in reactive protocols is carried out in two steps, viz. route discovery and rout maintenance. Dynamic Source Routing (DSR) and Ad-hoc on Demand Distance Vector (AODV) are examples of reactive (on-demand) routing protocols.

- **Ad-hoc On Demand Distance Vector (AODV):** It is reactive version of DSDV protocol that minimizes the required number of broadcast by creating on demand routes instead of maintaining complete list of routes as in DSDV. It uses destination sequence number to maintain up-to-date routes and DV logic in calculating the best suited path.
- **Dynamic Source Routing (DSR):** It is similar to AODV, except that in DSR nodes are required to maintain route caches that contains the source routes of which the node is aware. Route cache is updated as new routes are learned.

(iii) Hybrid Protocols*:* Hybrid routing protocols combine the good features of both proactive and reactive protocols. The hybrid protocols are designed to overcome increased scalability by allowing nodes to form some sort of a backbone (clusters) to reduce the route discovery overheads. This is mostly achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes only when required by using route discovery strategy e.g. Zone Routing Protocol (ZRP).

- **Zone Routing Protocol (ZRP):** It is a hybrid protocol. It incorporates the merits of both proactive and reactive routing protocols. A routing zone is similar to a cluster. A routing zone comprises a few MANET nodes within a few hops from the central zone. This implies that the regular route updates take place within the zone only. Each node has route to all other nodes within the zone. If the destination happens to be outside the zone, ZRP employs on-demand route discovery procedure.

Now we will explore applicability of MANETs.

1.2 Application of MANETs

There are so many applications of MANETs some of them are listed below [2]:

1.2.1 Tactical Networks:

Military communication and rescue operations.

1.2.2 Emergency Services:

Search and rescue operations, disaster recovery, replacement of fixed infrastructure in case of environmental disasters (like floods, earth quakes etc.), supporting doctors and nurses in hospitals, policing and firefighting.

1.2.3 Commercial and Civilian Environment:

E-commerce: Electronic payments anytime and anywhere.

1.2.4 Business:

Dynamic data base access and, mobile offices.

1.2.5 Vehicular Services:

Information about road and accident guidance, transmission of road and weather condition, taxi cab network, inter-vehicle networks.

1.2.6 Supports stadiums, Trade fairs, Shopping Malls.

1.2.7 Education

Universities and campus office settings, virtual class room, ad-hoc communication during meeting or lectures.

1.2.8 Entertainment

Multi user games and wireless P2P networking.

1.2.9 Sensor Networks

Home applications smart sensors and actuators embedded in consumer electronics includes, Body Area Network (BAN). A BAN, in place on a patient can alert the hospital, even before they have a heart attack, through measuring changes in their vital signs. A BAN on a diabetic patient could auto inject insulin through a pump, as soon as their insulin level declines.

Now we will explore mobile agents and their applicability in MANETs.

1.3 MANETS Feature and their Impact on Security

The features of MANETs that make them more vulnerable to attacks and misbehavior than traditional wired networks, and imposes the security solution to be different from those used in other networks. These features are as under:

1.3.1 Infrastructureless

Central servers, specialized hardware, and fixed infrastructures are necessarily absent in MANETs. The lack of infrastructure precludes the deployment of hierarchical host relationships. Instead, nodes uphold open relationships. That is, they assume contributory collaborative roles in the network rather than ones of dependence i.e. any security solution should rely on cooperative scheme instead of centralized one.

1.3.2 Wireless Links *Use*

The use of wireless links exposes a wireless ad hoc network susceptible to attacks. Unlike wired networks where a hacker must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Hence, a wireless ad hoc network will not have a clear line of defense, and every node must be prepared to threats. Moreover, since the channel is widely accessible, the MAC protocols used in ad hoc networks, such IEEE802.11 rely on trusted cooperation in a neighborhood to ensure channel access, which exposes MANETs to vulnerability.

1.3.3 Autonomy of Nodes

Mobile nodes are autonomous that can move independently and changes the topology of network dynamically. This means that tracking down a particular mobile node in a large scale ad hoc network cannot be done easily, and any security threat can take advantage of it.

1.3.4 Power Limitation

Ad hoc enabled mobile nodes are small and light weight, therefore they have limited power resources (battery) to ensure portability. This limitation causes vulnerability since a node powering-off can cause its break-down. Thereby, attackers may targets those nodes to disconnect them, even can make network partition. This is called energy starvation attack or sleep deprivation torture attack.

1.3.5 Memory and Less Processing Speed

Ad hoc enabled mobile nodes have limited storage and weak computational capabilities. High complexity security solutions employed, such as cryptography, should take these constraints into consideration.

1.4 Security Attacks in MANETs

The security attacks that can affect MANETs can be divided into two classes i.e Attacks and Misbehavior [12].

1.4.1 Attacks

Attacks are the actions that intentionally try to cause damage to the network. the attacks can be subdivided on the basis of their origin or nature. Further the origin based attacks are of categories external and internal. Whereas nature based splits them into active and passive attacks.

1.4.1.1 External Attacks

The attacks those are launched by a node that is not the part of logical network or is not allowed to access the network.

1.4.1.2 Internal Attacks

The attacks those are launched by the internal compromised or malicious node. It is more dangerous type of threat because the security mechanism towards external attacks is ineffective against the compromised and malicious nodes.

1.4.1.3 Passive attacks

A passive attack is the continuous collection of information that is further used for launching and active attack. The attacker eavesdrops the information being transferred (packets) and analysis it to extract required information from it. Due to the wireless nature of the communication medium this is open to access and easier for hacker to hack in this environment as compared to wired networks. The solution to this security issue is to use information confidentiality attribute [12].

1.4.1.4 Active Attacks

These are the attacks launched by actively interacting with victims such as:

- **Sleep deprivation torture:** In which batteries are targeted
- **Hijacking:** In this type the attacker controls the communication between two nodes and masquerades one of them.
- **Jamming:** Due to over using of channel that makes it unavailable communication nodes.
- These attacks result in Denial of Service (DoS) which results in complete failure of communication between nodes.
- **Sleep deprivation torture:** In which batteries are targeted
- **Hijacking:** In this type the attacker controls the communication between two nodes and masquerades one of them.
- **Jamming:** Due to over using of channel that makes it unavailable communication nodes.These attacks result in Denial of Service (DoS) which results in complete failure of communication between nodes.

1.5 Misbehavior

Misbehavior threat can be defined as an unauthorized behavior of an internal node that results in unintentionally damage to other nodes [12]. The intention of the node is not to attack but it may have other unfair advantage as contrast to others e.g. one node may deny to forward packets for other nodes to save its resources, while using their resources and asking them to forward on their own.
The security attacks that can affect MANETs can be divided into two classes i.e., Attacks and Misbehavior [12].

1.6 AODV Based Security

Ad hoc On Demand Distance Vector is based on distance vector routing protocol in MANETs. Security that is implemented in AODV is based on one-way hash, two-way hash and digital signature [17]. To secure message transmission in AODV an encryption algorithm with first key is used. In AODV protocol firstly the source node generates two signs with and without key. Second intermediate sign with a without key and then forwarded to the destination node. And then destination node generates sign with key and compares it with source node. After the comparison of the key value matches, destination node replies back to source node. Secure Hash Algorithm (SHA) is double layer security algorithm which is expandable, flexible and efficient.

1.7 Centralized Secure Routing Protocol (CSRP)

Centralized Secure Routing Protocol envisage mobile nodes (MN) and general nodes. MN in MANET environment act as third party and provide and protocol, and provides authentication between the nodes for communication purpose. CSRP maintains a session key between the source and destination nodes. In this mechanism a node sends request to the mobile node for creating session key with neighboring node. When trusted neighboring node is found it will reach the destination node, the destination node replies to source the source node by first request accepted by neighbor. This eradicates the flooding and makes the data transmission secure.

1.8 Link State Routing Security

In MANETs optimized Link State is a proactive routing protocol. In secure OLSR framework is designed to enhance the security in MANETs. In OLSR the best (Multi Point Rely)MPR selection is done by means of closing mechanism reachability of the node, to share the secret key threshold cryptographic technique is used and finally the shares reconstructed by using language interpolation method [17].

1.9 Aggregate Based Path Verification

The aggregate based path verification routing protocol (APVP) uses identity based cryptography and aggregate signature algorithm. The ID based cryptography generates a pair of keys with help of private key generator to identify the distinct users. The private key generator uses a secure path to send private key to the owner identify one of the keys are generated. In APVP the routing is secured by broadcasting the packet to the neighbor node. These secure route discovery packet (RDP) consists of identifier signature and the message to be sent with timestamp. When the node receives RDP message and sets the reverse path. Every node on the reverse path to the source sends the reply (RREP). The APVP secured routing provides the security property of validity, authentication and non-impersonation.

1.10 Cooperation of Nodes Fairness in Dynamic Ad Hoc Network (CONFIDANT)

The CONFIDANT protocol [18] is employed for detection and isolation of misbehaving nodes, the proposed protocols carries out the function by repudiation system. Where the trust and routing are calculated by experience, observation and behavior of the nodes in the network. In this protocol the misbehaving nodes are blacklisted and isolated from the network. The advantage of this protocol is that it can detect selfish and wormhole nodes and isolate them the system, which causes dropping of packets. The main limitation of the protocol is that the associated repudiation system fails to give any protection against false execution which results in blackmailing.

1.11 Security Aware Ad Hoc Routing (SAR)

The security aware Ad Hoc routing also kwon as SAR [19] in the proposed system SAR classifies the nodes on the basis of their trust values. On the basis of the classification the secret group key is shared among the nodes with same trust level. While choosing the route, the source node sets minimum number of security requirements which a node needs to fulfill to complete the routing path from sender to receiver. On addition the source node can agree making path by encryption of route request packets with some keys at specific levels. In the proposed system these keys can create problems when malicious node will hack the keys inspite of having high security while controlling secret group keys.

2. MOBILE AGENTS

Mobile Agents are special type of software agents, can be defined as autonomous executing programs that can halt themselves, migrate to another host, in a heterogeneous environment and continue execution without being affected by the status of the originating node. A software mobile agent can carry out tasks from one node to another in flexible and intelligent way as response to the new changes in the network. This gives the special ability to communicate with one another, learn from their experience and cooperate with each other.

2.1 Scope of Mobile Agents in Wireless Communication:

A Mobile Agent has a unique feature to move from one system to another in the same network. This ability allows it to move to a system containing an object with which it wants to interact and then to take advantage of being in the same host or network as the object. This is good reason for using mobile agents in wireless communication are [6]. Mobile Agents are useful in network management specially in diagnosing faulty nodes in MANETs [7][8]. Some of the features of mobile agents are as follows:

2.1.1 *Mobile Agents Reduce Network Load*: Mobile Agents allow users to package a conversation dispatch to a destination host where interactions take place locally. Mobile agents are useful in reducing the flow of raw data in the network. Data is processed in its locality rather than transferred over network. Move the computation to the data rather than the data to the computation is the main mantra.

2.1.2 *Overcome Network Latency:* Mobile agents offer a solution: they can be dispatched from a central controller to act locally and execute the controller's direction directly.

2.1.3 Encapsulate Protocols:

Mobile Agents can move to remote hosts to establish "Channels" based on preparatory protocols.

2.1.4 Execute Asynchronously and Autonomously:

In mobile devices tasks require continuously open connection between a mobile device and a fixed network**.** To maintain this connection is not technically and economically feasible, so the tasks are embedded in the Mobile Agents and are dispatched to the Network, then the Agents become independent of the process that created them and can execute asynchronously and autonomously, and mobile device can be later reconnected to receive its Agent.

2.1.5 *Heterogeneous In Nature:* Mobile Agents are heterogeneous from both hardware and software point of view. They are computer and transport layer independent (Dependent on only there execution environment), they provide optimal condition for seamless integration.

2.1.6 *Robust and Fault Tolerant:* Ability of Mobile agents to react in unfavorable conditions and events makes them appealing for building robust and fault tolerant distributed systems. Thus they can be useful for dynamic topology changes in MANETs [8].

Typical advantages of using mobile agents in wireless environment include bandwidth conservation, reduced latency, load balancing, intrusion detection etc. The route of a mobile agent can be decided by its owner or it may decide its next Hop destination on the move on its own.

3. AGENT BASED MECHANISM IN MANETS

3.1 Master Directed Incentive Based Approach (MDIA)

It is the mechanism to detain selfish behavior of nodes in MANETs. The proposed approach MDIA [13] intends to find out the emerging selfish behavior between the nodes and detains the selfish behavior by motivating the nodes with low energy resources. It proposes that every node in the MANETs loaded with mobile agent for network formation and collaboration. The agents embedded in the participating node may play the role of master agent or mobile node agent. When the source node initiates the communication it becomes the master node for some time till the new master node is elected and the new elected node agent over takes the role of master agent. Master agent is liable for the following periodical jobs:

- Refreshing of energy table.
- Analysis of packet info table of nodes.
- Preparation of dynamic routing table and detaining selfish behavior and energy starving nodes by sending packets in 2:1 ratio.
- Updating incentive table.

The proposed system has two main parts i-e selection of master node and detecting critical nodes and detaining selfish behavior. The selection of master node is done by the mobile agent which checks the energy levels by traveling to the neighboring nodes. The node having highest energy level is elected as the master node.

3.2. Mobile Agents to Improve Quality of Service (QoS) in MANETs and VNAETs

QoS is the main motive of network to be offered by the network to the user. Mobile Agent can provide deterministic performance so that the information and resources could be better utilized. Due to the characteristics if mobile agents discussed earlier, Agents can be used in MANETs and VANETs according to the literature survey so many issues have been answered in the MANETs and VANETs to deliver better QoS and some of the issues are yet to be answered [10]:

- Lack of real time Traffic Info.
- Lack of real time 24 hour alternate routes info.

3.3 Mobile Agents for Intrusion Detection

[9] Intrusion Detection System is a protection system that automatically diagnosis intrusion and malicious behavior within the node or network and then reports for subsequent actions. IDS can work on host level or network level thus becoming host based or network based respectively.

The literature survey highlights a number of Intrusion Detection Systems in MANETs few listed in this paper.

3.3.1 LIDS (Local Intrusion Detection System)

In LIDS the MAs running on different nodes jointly work in preparing complete intrusion picture. The framework depends on the edge provides by Simple Network Management Protocol (SNMP). The data used, which is stored in Management Information Base of SNMP [14].

3.3.2 Intrusion Detection System Based on Static Stationary Database

The proposed architecture of the IDS comprises of two parts Mobile IDS agents that run on every node and a secure database that maintains global signature. If known misuse attacks and stores pattern of each of every node's normal activity in a non-hostile environment. The proposed IDS agents' responsibility is to detect intrusion based on local audit data and take part in cooperative algorithms with other IDS agent to decide on attacks [1].

3.3.3 Distributed Intrusion Detection Using Mobile Agent

The system is non monolithic one that uses several sensor types performing different functions. Every module epitomize a lightweight mobile agent with certain functionality. This helps in making network lighter by dividing the functional tasks into categories and assigning an agent to a specific task. In addition to this mobile agent in this framework facilitates sensor's mobility and the intelligent routing of intrusion data through MANETs [16].

4. CONCLUSION

The survey provides the sketch of MANETs, its uses, working, security issues and challenges, the different protocols discussed and the security mechanism in these protocols. The different protocols discussed try to overcome these security challenges, but still so many security issues are open for researchers to work. Use of mobile agents discussed tries to eradicate some issues to some extent. And future research in Mobile Agent uses in MANETs can be can used in key distribution and cryptographic solutions. The literature survey suggests that mobile agents could be handy in MANETs in finding solutions to different security issues. The different security issues such as trust management, spoofing, denial of service, tracking down of malicious node issues needs to be take care of while designing MANET routing protocols.

5. REFERENCES

[1] P. K Pattnaik and Rajib Mall, "Fundamentals of Mobile Computing", PHI Learning Pvt. Ltd., 2nd Edition, 2014.

[2] Hoebeke Jeroen, Ingrid Moerman, Bart Dhoedt, and Piet Demeester, "An overview of Mobile Ad Hoc Networks: Applications and challenges", Journal Communications Network 3, no. 3, 2004, pp. 60-66.

[3] D. Fife Leslie and Le Gruenwald, "Research issues for data communication in Mobile Ad Hoc Network database systems", ACM SIGMOD Record 32, no. 2, 2003, pp. 42-47.

[4] Shen, Wei-Liang, Chen Chung Shiuan, Kate Ching-Ju Lin, and Kien A. Hua. "Autonomous Mobile Mesh Networks", Mobile Computing, IEEE Transactions on 13, no. 2, 2014, pp. 364-376.

[5] Shakshuki Elhadi M., Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs." Industrial Electronics, IEEE Transactions on 60, no. 3, 2013, pp. 1089-1098.

[6] Lange, Danny B. and Mitsuru Oshima, "Seven good reasons for mobile agents", Communications of the ACM 42. 3, 1999, pp. 88-89.

[7] Bieszczad Andrzej, Bernard Pagurek, and Tony White, "Mobile agents for network management", Communications Surveys & Tutorials, IEEE 1, no. 1, 1998, pp. 2-9.

[8] Roy, Debdutta Barman, and Rituparna Chaki, "MADSN: Mobile Agent Based Detection of Selfish Node in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, 2011, pp. 225-235.

[9] Hijazi, Abdulrahman, and Nidal Nasser, "Using mobile agents for intrusion detection in wireless ad hoc networks", In Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference on Networks, IEEE, 2005, pp. 362-366.

[10] Kumar, Rakesh, and Mayank Dave. "Mobile agent as an approach to improve QoS in vehicular ad hoc network", IJCA Special Issue on Mobile Ad-hoc Networks, MANETs, 2011, pp. 67-72.

[11] Joshi Praveen, "Security Issues in Routing Protocols in MANETS at Network Layer", Procedia Computer Science 3, 2011, pp. 954-960.

[12] Djenouri Djamel, LyesKhelladi and Nadjib Badache. "A Survey of Security Issues in Mobile Ad Hoc Networks", IEEE Communications Surveys 7, No. 4, 2005, pp. 2-28.

[13] Singh, Aarti, and Divya Chadha. "MDIA-Master Directed Incentive Based Approach", International Journal of Computing Academic Research(IJCAR), Volume 2,Number 6, December 2013, pp. 255-265.

[14] P. Albers et al., "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," 1st Int'l. Wksp. Wireless Info. Sys., Ciudad Real, Spain, Apr. 3–6, 2002.

[15] A. B. Smith, "An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks," 5th Nat'l. Colloq. for Info. Sys. Sec. Edu, May 2001.

[16] O. Kachirski and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks," Knowledge Media Net., Proc. IEEE Wksp., July 10–12, 2002, pp. 153–58.

[17] S Balasubramani, S. K. Rani, K. SujaRajeswari Review on Security Attacks and Mechanism in VANET and MANET" Artificial Intelligence and Evolutionary Computations in Engineering Systems Volume 394 of the series Advances in Intelligent Systems and Computing pp 655-666

[18] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDENT Protocol," in Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), June, 2002, pp. 226-236.

[19] A. Majumdar and S. Banerjee, "Different secured routing protocols for mobile Ad Hoc networks and its vulnerabilities: A review," Computing and Communication (IEMCON), 2015 International Conference and Workshop on, Vancouver, BC, 2015, pp. 1-5.