Middle-East Journal of Scientific Research 24 (10): 3094-3107, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.3094.3107

# MANET – A Cogitation of its Design and Security Issues

[1]Rashidah F. Olanrewaju, [1]Burhan Ul Islam Khan, [1]Farhat Anwar,
[2]Abdul Raouf Khan, [1]Faraz Ahmed Shaikh and [3]Mohammad Shuaib Mir

[1]Department of Electrical & Computer Engineering, Kulliyyah of Engineering,
International Islamic University Malaysia, Kualalumpur, Malaysia
[2]Department of Computer Sciences, King Faisal University, Saudi Arabia
[3]Department of Information Systems, Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia, Kualalumpur, Malaysia

**Abstract:** With the fast proliferation of wireless devices e.g., cell phones, PDAs, laptops, wireless sensors, etc., the significance of wireless communication especially mobile adhoc networking is quite evident. The need to shun dependency on fixed infrastructure networks led to the evolution of Mobile Adhoc Network (MANET). MANETs have numerous advantages like dynamic topology, lack of centralization, speedy and affordable installation, etc. but the features of MANETs impart certain complications as well such as unreliability caused due to node mobility, bandwidth constraints of the wireless link making it vulnerable to attacks, lack of standardization of security solutions, etc. Notably, security in MANETs is a challenge to researchers. In this paper, an overview of MANETs is provided followed by a critical account of the relevant review work that has been carried out so far in this domain. This paper tries to highlight the various issues in the design and security requirements of MANETs. As such, the proposed study revolves around all the security aspects of mobile adhoc networks including routing protocols, mobile agents, malicious nodes, intrusion detection system and other factors that affect the quality of service in MANETs.

**Key words:** MANET · Mobile agent · MANET security · Node misbehavior · IDS

## INTRODUCTION

In the current era, the wireless communication technology has evolved as one of the most empowering and transforming technologies, especially the study of Mobile Adhoc Networks (MANETs) has been the most popular [1, 2]. It was Internet Engineering Task Force (IETF) who proposed the term Mobile Adhoc Network for the first time in 2002 [3]. MANET is a communication network that is infrastructure-less [4]. Infrastructure-less network means one that does not have pre-existing infrastructure i.e. base stations and access points. In other words, the network infrastructure of MANET is decentralized i.e. it has no need of a fixed infrastructure due to which the nodes in MANETs can move in a random fashion. MANETs have the capability to create self maintaining and self configuring a network devoid of a centralized infrastructure support which makes it is suitable for widespread applications in critical fields such as emergency recovery, military conflicts, disaster recovery, etc. [5]. The mobile nodes in a MANET are provided with wireless transmitter/receiver and the neighbourhood of the nodes in the network is defined by their radio range. A node can simply make use of a broadcast for establishing communication link with its neighbouring nodes but the radio range is reduced by interference and energy consumption. Since the nodes have a restricted range, the ones that are out of range need to rely on intermediate nodes; the intermediate nodes act as routers. Such type of network is called Store-and-Forward (or Multi-Hop) network [6]. The intermediate nodes are responsible for discovering and maintaining routes towards other nodes. A node within the network can be located anywhere say, extremely small devices, in/on cars, trucks, aero planes, ships or on people as well.

A mobile adhoc network is an adaptive and self-organizing network which implies on the fly deformation of a formed network with no requirement of system administration. Such an infrastructure less network comprises of enormous number of nodes which form way for a communication link to other nodes in the network thus giving rise to numerous mobile nodes [7-9]. There are

**Corresponding Author:** Burhan Khan, Department of Electrical & Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia, Kualalumpur, Malaysia.

several security loopholes in mobile adhoc networks like limited physical security, lack of infrastructure, dynamic topology and resource constraints [8, 10]. As a result of these loopholes, there also arise QoS issues in MANETs such as routing, energy, bandwidth, etc. which further lead to possibilities of attacks on mobile adhoc networks [10].

The dynamic topology and decentralization of MANETs pose a major challenge to the formulation of security for MANET system. The routing protocols therefore have to make a random selection for communicating in MANETs giving rise to one of the important security issues viz. authentication of genuine and malicious nodes. Existence of any kind of malicious node in a MANET is detrimental for any of the applications of MANETs and causes huge loss to the resources connected to the network [8, 11].

The distinctive feature of a MANET is its self configuration property by virtue of which it is able to operate in a decentralized way without relying on any centralized managers such as access points or base stations. Generally, each and every node in a mobile adhoc network functions as a router for accomplishing the objective of wireless communication among all the nodes in the network including even those located distantly. In such type of communication network, a framework should be set up for multi hop channels in a defined functional scenario or in some reactive or proactive method and in order to achieve this, routing behaviour largely depends on Medium Access Control (MAC) layer in OSI model. Thus, such networks are shrouded with issues that are found in the conventional wireless communication system e.g., hidden/exposed terminals. A MANET adopts multi-hop communication strategy for connecting the remote nodes and channels in the network.

However, due to its dynamic and decentralized nature, there arises a great deal of congestion in the network. In general, congestion in such a communication system brings about regeneration as well as data drop reflecting the substandard optimization of network resources thereby leading to degradation in QoS [12]. Moreover, due to network overhead arising from node mobility, node link and limited available resources, facilitating requirements of end- to-end performance happens to be irksome. Numerous systems have been put forward for optimizing the QoS in MANETs after taking into consideration the various approaches and paradigms. Providing quality in MANETs can be made possible by allocating or managing resources efficiently, enhancing lifetime of network and routing optimally for ensuring uninterrupted data transmission. All the goals mentioned can be achieved efficiently by optimization of MAC layer in OSI model which can take an important part in optimizing QoS of mobile adhoc networks [13].

**A. Characteristics of MANETs:** The mobile nodes or devices in MANETs with networking potentiality are able to communicate with one another quite easily. Those devices can be mobile phones, sensors, laptops, GPS, palmtops, etc. The various characteristic features of MANETs have been elucidated below:

***(A1)Distributed Operation:*** In MANETs, every node acts as a host as well as a router i.e., it shows self-sufficient behaviour. MANETs exhibit distributed operation in routing, host configuration and security.

***(A2)Multi-hop Routing:*** MANETs possess the capability of multi hop routing which is employed for communication between nodes when they are beyond each other's radio range i.e., there are intermediate nodes acting as routers which forward and relay packets.

***(A3)Dynamic Topology:*** The various nodes in a MANET have the capability of joining or leaving the network at any point of time thereby leading to a dynamic kind of topology in MANETs. The nodes left can later form a new network.

***(A4)Light-weight Terminals:*** Nodes in a MANET possess light weight characteristics, reduced processing speed, power and memory. Therefore, they are also known as thin clients.

***(A5)Autonomous Establishment:*** The behaviour of MANETs is spontaneous and mobile that calls for least possible human involvement for network configuration. Moreover, they can have large user mobility plus huge user density.

***(A6)Speed:*** There is not any requirement of extra hardware/software for setting-up a mobile adhoc network, though some changes in settings may be done. MANET is ideally suitable in situations when several nodes need to be connected to a network effortlessly and in a short span of time.

***(A7)Router Free:*** The services of a router are not required when nodes are to be connected to a MANET. As a result, it is more reasonable to run a mobile adhoc network as compared to conventional networks.

***(A8)Mobility:*** In MANETs, the nodes are free to move in any random direction and routing protocols deal with the issues pertaining to node mobility.

***(A9)Connectivity:*** All the nodes in the network collaborate with each other for packet delivery to their respective destinations which is a consequence of decentralization in MANETs.

***(A10)Fast Installation:*** Since MANETs do not require access points or base stations, their installation is remarkably flexible. Furthermore, they take little time to install which can prove a boon in times of natural disasters such as earthquakes, floods, etc.

***(A11)Cost:*** Owing to the elimination of costs incurred by fixed infrastructure and less power consumption, MANETs have been found to be economical and cost-effective in certain situations in comparison to traditional networks.

***(A12)Fault Tolerance:*** The various transmission protocols and routing in MANETs are capable enough to provide support in case of connection failures.

**B. Topology in MANETs:** There are no hard and fast rules for topology in MANETs. The MANET topology is dynamic in nature that means the topology changes dynamically for several causes. Whenever nodes dislocate and go beyond the radio range of other nodes in order to establish connection with new nodes, there is a change in MANET topology. Furthermore, there may be modification in logical topology in fixed adhoc networks such as, wireless sensor fields because of restricted bandwidth or wireless link when caused to experience jamming and fading or when the nodes are damaged by hostile condition or battery discharging.

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

**C. Protocols in MANETs:** Protocols are set of rules and regulations that govern the smooth communication between the communicating devices. The protocols followed by MANETs can be categorized into two types: i) Proactive and ii) Reactive.

***(C1)Proactive Protocols:*** In proactive protocols, the nodes maintain entire routing information of the network in a table beforehand, even without demand e.g., Cluster-head Gateway Switching Routing (CGSR), Destination Sequenced Distance Vector (DSDV), etc. The approach followed by the protocols is to seek an optimal path [14].

***(C1a)Destination Sequenced Distance Vector (DSDV):*** This protocol is the one of the most primitive protocols in mobile adhoc networks. It is based on distributed Bellman Ford routing scheme. In DSDV, every node keeps up a routing table which stores the number of hops to every destination node together with the neighbor that is on the subsequent hop along that route. Then, updated routing tables are maintained by the surrounding nodes amongst themselves.

***(C1b)Cluster-head Gateway Switching Vector (CGSR):*** The nodes in hierarchical networks are present in the form of clusters and a special node heads the cluster; this special node is referred to as cluster-head. The special nodes selected as cluster-heads are part of separate clusters and operate as gateways amongst the clusters.

***(C2)Reactive Protocols:*** Reactive protocols collect the required routing information unambiguously provided that is required for sustaining a genuine session. Generally, routing protocols carry out routing in two distinct phases namely route discovery and route maintenance. Ad-hoc On-demand Distance Vector (AODV), Associative Based Routing, Dynamic Source Routing (DSR), Tiny Ad-hoc Routing Protocol (TARP) and Temporally Ordered Routing Algorithm (TORA) exemplify reactive routing protocols [14].

***(C2a)Ad-hoc On Demand Distance Vector (AODV):*** This protocol is identical to DSDV protocol with the only difference that routes are created on-demand rather than maintenance of the entire route list in the network, thereby minimizing the number of broadcasts needed. The best suitable route is calculated with the help of Distance Vector (DV) logic and destination sequence number is used for keeping the routes updated.

***(C2b)Dynamic Source Routing (DSR):*** It is the same as AODV with the exception that route caches have to be maintained by nodes in DSR which store only those source routes that are known to the node. When new routes are found, the route cache is brought up to date.

***(C3)Hybrid Protocols:*** These protocols are a combination of good attributes of reactive as well as proactive protocols. The main goal of designing these protocols is to decrease overheads associated with route discovery arising as a result of the enhanced scalability which is brought about by grouping nodes in certain kind of a backbone (such as clusters). In order to achieve this, the routes to nodes in close proximity are maintained proactively whereas the routes to distant nodes are determined by route discovery mechanism only when demanded. An example of such a protocol is Zone Routing Protocol (ZRP).

***(C3a)Zone Routing Protocol (ZRP):*** Routing zones are analogous to clusters. Several nodes of mobile adhoc networks that come in the range of few hops from central zone form a routing zone. This means that routes are updated regularly within that zone i.e., there is a route between every pair of nodes inside the zone only. However, if destination node lies external to the zone, Zone Routing Protocol makes use of on demand route discovery mechanism.

Besides the above mentioned protocols, there is another routing protocol which is known as Geographic or Location-based routing protocol. The main purpose of this protocol is elimination of flooding. In such a type of protocol scheme, the potential estimated information of the location coordinates of source node, its neighbouring nodes and destination node determine the subsequent hop in the path to its destination. There is no need of establishing and maintaining routes thereby resulting in efficient utilization of the network resources. Examples of such protocol are guaranteed delivery routing, limited flooding-based routing and progress-based routing [14].

**D. Applications of MANETs:** MANETs are supposed to be useful in disaster recovery, battle field communications and rescue operations where infra structured networks do not exist or got damaged due to disaster [3, 7, 15, 16]. It is feasible means for ground communication and information sharing. MANETs have lots of applications some of which have been given below:

***(D1)Emergency Service:*** MANETs provide support in case of disaster recovery, rescue operation, military communication, replacing fixed infrastructure in times of natural disaster such as earthquakes, floods, etc., fire fighting, policing and aiding doctors/nurses in hospitals.

***(D2)Commercial/Civilian Environment:*** Another important application of MANETs is e-commerce and electronic payments can be done anytime, anywhere. MANETs have their applications in trade fairs, sports stadiums, shopping malls, etc.

***(D3)Business:*** MANETs provide access to dynamic data base and mobile offices have been made possible.

***(D4)Vehicular Service:*** MANETs can provide guidance about roads or accidents, information about weather and roads can be transmitted and there is also taxi cab network and inter-vehicle networking.

***(D5)Education:*** Mobile adhoc network set-ups are found in university campus settings. Virtual classrooms and communicating in an adhoc manner during lectures or meetings is a reality because of MANETs.

***(D6)Entertainment:*** Wireless peer-to-peer networks and multiple-user gaming are some of the applications of MANETs that provide entertainment.

***(D7)Sensor Networks:*** Home applications, actuators and smart sensors are embedded in consumer electronics, e.g., Body Area Network (BAN) [17]. Such a network when placed on a patient has the ability to alert the hospital of a heart attack, even before encountering one, by measurement of changes in their crucial signs. In the same way, a BAN can inject insulin into a diabetic patient autonomously via a pump whenever there is a decline in the level of insulin.

**E. Security issues in MANETs:** A mobile adhoc network or popularly known as MANET has been the constant focus of the research community due to its potential communication capability using mobile devices. In MANET, the mobile device acts itself as an individual router and thereby tends to move in independent direction. Owing to dynamic topology of nodes all the QoS issues as well as security issues arise in MANET. Although, various QoS issues e.g., bandwidth, latency, packet delivery ratio, etc. have witnessed an extensive study in the past, but security problems inevitably are yet to see some standard and remarkable outcome. Due to dynamic topology, such adhoc network encounters frequently intermittent link that affects the communication immensely. Owing to the decentralized nature of the network, MANET security system poses a higher dimensional challenging with respect to authentication and authorization. One of the complex security problems in MANET is to visualize the behaviour of node, which may be any type of computing devices e.g. laptop, tablet PC, smart-phone etc [18].

Various cryptographic based studies have been conducted in the past to provide better security. However, more or less every prior study considers certain case study of attack scenario and then deploys formulation of attack mitigation model. One of the disadvantage of such study is that the countermeasures techniques are highly specific and is not applicable when the adversarial scenario changes. Hence, it is important that before formulating a new mitigation technique against the security issues of MANET, the node misbehaviour problems should be investigated properly as it is one of the complex studies. Understanding the behaviour of various kinds of nodes in a MANET system will enable the researcher to closely visualize the pattern of attacks and attacking strategy. It will also assist the researcher to visualize how far their mitigation technique will be successful on a selected attack scenario. Hence, better security protocol can be designed cost effectively if the exact behaviour of the node be extracted empirically [19].

Owing to frequent topology changes, tactical applications, decentralized infrastructure and nomadic computing, several issues arise in MANET security which should be taken into consideration for proper deployment [20].

Mobile adhoc networks are susceptible to malicious behaviour. Absence of certification authority and centralized infrastructure is the main cause of MANET vulnerability to interference, eavesdropping, infiltration, etc. Security in mobile adhoc networks is considered to be the main road-block in applications of the networking technology in business [21]. However, in MANETs, the security requirements are dependent on the application areas where they are set up. For example, in emergency or military operations, the network needs to be safeguarded from external interferences whereas the networks in commercial applications may get compromised if the nodes fail to cooperate. The nodes in MANETs can enter and leave anytime and there are chances that channels transfer data through nodes which are not genuine. Thus, there should be some criteria that define membership of nodes in MANETs and the basis of classifying trusted and non-trusted nodes.

The methods presently in use for securing data by cryptographic techniques present a challenge in the form of refreshing the network periodically and key distribution. The most severe dilemma is the possibility of a node getting compromised or captured. As a result, such a node when given access to structural information in the network can relay data but at the same time it may cripple the whole network in no time by sending fallacious routing information.

**F. Security Attacks in MANETs:** The security attacks in MANETs can be classified as [22]:

- Passive Attack
- Active Attack

**(*F1*)Passive Attack:** In this attack, there is no disruption in the protocol operation however there is an attempt to learn important information by eavesdropping on network traffic.

**(*F2*)Active Attack:** Active attack attempts to disrupt protocol operation by injecting arbitrary packets with the aim to acquire authentication, restrict availability or draw packets that are meant to be delivered to other nodes.

The protocols used for routing in MANETs are found to be vulnerable to attackers because they can access the information about topology of network quite easily [23].

- **(*F2a*)Attacks using Modification:** One of the easiest methods employed by malicious nodes to disrupt the sound working of mobile adhoc network is the announcement of a better route than other routes. The basis of such an attack is alteration in the metric values of routes or message control fields.
- **(*F2b*)Attack using Impersonation:** Such kind of attack is also known as spoofing because the actual IP addresses or MAC addresses are not used by malicious nodes rather they are kept hidden. Since the source IP address is not authenticated in existing routing protocols such as DSR, AODV, malicious nodes can launch several attacks by means of spoofing.
- **(*F2c*)Attack using Fabrication:** This attack can also be referred to as counterfeiting. In this attack, authentication checks are bypassed and information is impersonated. Generally, additional information is appended in a file in this kind of attack. The main objective in this attack is gaining access to any service or data.

**G. Mobile Agents in MANETs:** In order to tackle the issues associated with MANETs, mobile agents can be used, e.g., MANETs undergo typical topology changes because nodes are free to move, this topology change disrupts information flowing over the pre-defined paths. Nowadays, MANETs are employed for a variety of uses like intrusion detection, network detection, proper bandwidth utilization, service discovery, automatic network reorganization, etc.

Mobile agents are special type of software agents and may be described as independently executing programs which have the capability of halting themselves, then migrating to different hosts, present in heterogeneous environments and continuing execution with no involvement of source node status [24]. In response to further modifications in network, software agents are used for performing tasks of all the nodes in an intelligent and flexible manner. In this way, mobile agents help nodes in communicating with each other, collaborate with one another and learn from past experiences [25].

Mobile agents have the distinctive characteristic to move between different systems in a network. With this ability, it is possible for mobile agents to shift to the system that has the required object and benefit from being present in the same network or host. An important reason to use mobile agents for wireless communication technology [26] is considered to be their usefulness in network management in diagnosing faulty nodes in MANETs. Mobile agents are characterised by the following properties:

**(a)Reduction in Network Load:** Users are allowed to package the conversation to be dispatched meant for a particular destination where local interactions occur. Mobile agents have been found to be particularly beneficial when raw data flow is to be reduced in the network. Data is processed in its locality and not transferred on the network. Thus, the principle followed is the movement of computation to data instead of moving data to computation.

**(b)Solution to Network Latency:** Mobile agents present a solution to the problem of network latency by their ability to get dispatched from a central manager in order to perform execution of their directions locally.

**(c)Encapsulation of Protocols:** On the basis of preparatory protocols, mobile agents are able to shift to distant hosts for establishment of channels.

**(d)Asynchronous and Autonomous Execution:** In case of mobile devices, the related tasks require a connection between the device and the static network that should be open continually. Maintenance of such a connection is not feasible technically or economically, therefore, tasks are dispatched to MANETs after embedding them in mobile agents. In this way, the mobile agents operate autonomously and asynchronously without dependence on the processes that generated them. Later, the mobile device can be connected once again for receiving the mobile agent.

**(e)Dynamic Adoption:** Mobile agents can distribute themselves among the variety of hosts present in the network for maintaining optimal configuration to solve a specific problem.

**(f)Naturally Heterogeneous:** Mobile agents are heterogeneous from hardware as well as software aspect. They are independent of both computer and transport layer i.e., they depend on their execution environment only. Thus, they offer optimal condition for faultless integration.

**(g)Robustness and Fault Tolerance:** Mobile agents are able to respond to unfavourable events and situations making them feasible for building fault-tolerant and robust distributed systems.

Typical advantages of employing mobile agents comprise of load balancing, bandwidth conservation, reduced latency, etc. Furthermore, the owner of mobile agent decides its route or the next-hop destination may be decided dynamically by the agent itself.

The rest of the paper is organized as follows: Section II is entirely devoted to the study of relevant literature in the field of MANETs. The performance and security of MANETs has been focussed and the challenges found in existing review work have been put in Section III. Finally, the paper has been concluded in Section IV followed by the reference section.

## LITERATURE REVIEW

This section accentuates the review work carried out by eminent researchers in the domain of mobile adhoc networks together with the issues pertaining to them which are yet to be addressed.

The author [27] in his article has presented a survey on the present status and future research directions in adhoc networks to explore the issues that need research attention. Adhoc networks are found to operate as self-reliant independent networks that provide internal connections in a group. And in future, the demand could rise in such situations as military applications, shared desktop meeting or disaster recovery. Nevertheless, no significant applications of this technology have been identified. The author has also highlighted the research issues that need to be addressed which include scalability, power regulation, node cooperation, security, interoperability with internet and support for various protocols.

Authors in [28] have shown different milestones, challenges and research directions. They have categorized different types of MANETs according to current needs of today's world such as mesh networking, sensor networks, opportunistic networks, vehicular networks, people centric revolution. They have also given the applications of these sub-categories of MANETs. The different research issues in these networks are quality of service (QoS), performance optimization, reliable broadcast protocols and standardization, privacy and architectures.

In [29] authors have surveyed the strategies of transfer relay and congestion control in special type of MANETs called opportunistic networks. The modified version of TCP proposed for MANETs has been found ineffective in opportunistic networks. Their survey shows that reliable message delivery is still in early stage of development and needs focus of researchers.

In [15] authors have proposed EAACK (Enhanced Adaptive Acknowledge) especially for MANETs for intrusion detection as the MANETs are prone to malicious attacks. In comparison to other intrusion approaches, EAACK has demonstrated higher rates of detecting malicious behaviour in some instances and have zero effect on the performance of the network. EAACK has tackled three watchdog weaknesses viz. limited transmission issue, receiver collision and false misbehaviour. The proposed has been tested on simulations. It has a drawback that while incorporating digital signature in experiments, more routing overheads were generated. The future work can test it in real network environments and remove those routing overheads in incorporating digital signatures.

The author [30] in his article has written about the MANETs that they are growing fast and research is ongoing. MANETs have been found to play a significant role in railway applications as well as research efforts associated with it viz. Global Mobile Information System (GloMo). These networks provide users ubiquitous computing and information access. But the arguments that the MANETs are totally flawed architecture; the reason for that is MANETs are never used in practice. The wireless networks are still access point or base station related. The author has put forward the issues that make it flawed architecture and need to be addressed by researchers. The different issues are security, routing protocols, energy consumption.

In [31] author has given a review on a collection of ant colony algorithms which monitor traffic and provides an optimal solution of good path between the communicating nodes, as the vital challenge in MANETs is finding shortest path. The author has also discussed the general principles and applications of swarm intelligence routing. Furthermore, author has suggested that these algorithms give promising results but should be implemented very carefully.

Authors [32] in their paper have given the significance of Ad-hoc Networks. They have explored the different advantages and disadvantages of MANETs. Also, they have given different application areas of MANETs and have explored research issues that need proper attention of researchers.

Authors in [33] have explored and given definition, applications, characteristic problems and promises of software agents. They have suggested the future research areas needed for the advancement of software agents. And software agents cannot magically solve all the difficult problems.

In [34], the authors have explored their views about mobile agents, their classifications and capabilities. The basic concept about agents is message passing, agent communication, benefits and applications of mobile agents, agent languages and systems. In the challenges faced, mobile agents have mentioned security, control structures and transactional support.

Authors in [35] explored the prospective utilization of mobile agents in managing networks. They have ascertained that the mobile agents are useful in OSI management, network modelling and fault management (network diagnosis, remote maintenance of heterogeneous elements), configuration management and performance management.

In [36] authors have explored the main security threats to MANETs and the use of mobile agents that can help in challenging those security issues. Their analysis show great and promising suitability for a mobile agent based solution for intrusion detection systems to be adopted by MANETs. And their future vision is to design mobile agents to pull off maximum advantages from MANETs.

The authors in [37] have explored about the mobile agents, their security and issues. They have also given the desirable goals of mobile agents, the familiar techniques that can be fundamental in achieving distributing security. Security issues need proper future attention of researchers.

Authors in [38] have elaborated that energy efficiency is an imperative issue in MANETs as the energy supplies are stored in cells. It is important to maximize the minimum energy required by the node for data transmission to increase the network endurance. In their paper, they have presented an algorithm based on nature inspired Ant Colony Optimization structure for improving the energy efficiency in MANETs and thus helping in increasing overall lifetime of communication system.

In [39] authors have presented congestion control that occurs with limited resources. The standard TCP congestion is not capable enough to handle the distinctive features of a shared wireless channel. TCP congestion control gets problematic for MANETs. In order to ward off ad-hoc network congestion, a congestion control technique based on mobile agent has been proposed.

The system of MANET is beheld with various technical impediments owing to its inherent dynamic topologies. Although there are abundant volumes of research work, but the author [19] is of the view that very few have been able to effectively address the node misbehaviour problems in MANETs. This paper initially tries to draw a line between different types of nodes in MANETs based on their behaviour characteristics, then reviews some of the significant contribution of the prior researches for addressing node misbehaviour issues. A major emphasis is laid on the researches which use game theory as a tool to study and address the misbehaviour problems. The manuscript is developed considering some of the latest and standard evidences of past 5 years and finally discusses the open issues related to the problems. The outcome of the study is that although there are quite few researches works that have been carried out to counter the problem of node misbehaviour, but there still exist the wide range of open issues that need to be taken for mitigating the same completely especially the concurrent consideration of selfish and malicious nodes in the network while designing a extenuation technique.

Several solutions have been put forward to address the issues in MANETs however the solutions that have been provided so far for mitigation of security threats in mobile adhoc networks have not been standardized up till now or are deficient in robustness. A reason for this is the highly unpredictable nature of mobile nodes in MANETs that can be either regular or erroneous or malicious nodes. In [8] authors have elucidated the malicious behavior of nodes in detail along with assessment of different security mechanisms in place to mitigate the same. They present a review of the standard security techniques that have been taken up in most of the existing research works. The various security techniques have been discussed in view of their application in cryptography, intrusion detection systems, trusted third parties and other systems. Most of the methods have been found to employ cryptography for security purposes that is never devoid of drawbacks. The results obtained from the research conducted show that almost all the techniques employed focus on malicious node but there is no attempt to understand its basic pattern. The authors have encouraged the classification of nodes as malicious, selfish and erroneous as challenging where most of the potentialities of IDS systems discussed get down on their knees.Authors conclude that malicious nodes can present abnormal behaviour in their mobility also, however no security technique in this paper has considered this issue in any of their test-beds.

The paper [10] puts emphasis on the usage of probability theory and game theory by taking into consideration selfish nodes among a group of regular nodes and representing malicious versus regular node game thus making enhancement in the existing mathematical schema of tactical decision making for accommodating the same. The paper presents a framework representing the variety of random actions of node declination, node cooperation, node reporting and node attacks, all of which replicate tactical profiling of several mobile nodes. The authors have particularly concentrated on PBE strategy that forms the origin of the entire result analysis. On comparing the proposed work with the existing work, improvement has been depicted in terms of reduction in false positives by 63% that promotes overall utility of the network with erroneous as well as selfish nodes present in the same network. The main objective of the paper is to perform an analysis statistically and then construct mathematical model illustrating the tussle between malicious and regular nodes under varied susceptible security conditions considering the disparity in node collaboration by selfish and erroneous nodes inside the regular node camp. However, the framework proposed has not taken into account identification or detection of a particular malicious node in the simulation environment though quantified and cumulative empirical results of malicious behaviour have been extracted. The authors are of the view to present a combination of the proposed work and the prevailing credit-based method in the form of intrusion detection system as a future prospect.

The authors in [13] have proposed hybrid cross-layered scheme for MAC optimization in MANETs for achieving optimum energy conservation and resource sharing in real-time applications. The paper has illustrated the optimization approach called ElePSO built on the behaviour of elephant swarm for optimizing throughput and lifetime of node. The various features of elephant swarm behaviour like instantaneous reaction, sensitivity to surroundings and exceptional memorization have been contrived as optimized assignment of slots, identification of stable links and nodes and traffic-sensitive flexible scheduling in MANETs. ElePSO and TDMA-MAC have been integrated for ensuring energy-aware communication because CSMA/CA fails for multi-hop transmission of data. The results obtained after simulation reveal that the proposed ElePSO performs better than the existing bio-inspired optimization schemes viz. Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO). ElePSO shows higher number of active nodes with reduced communication overhead in comparison to ACO and PSO. The proposed scheme has proved to be a promising candidate for adhoc communication particularly for mobile nodes operated by battery. However, there is a scope for exploring the optimization of the system further in terms of heterogeneity and security of network together with higher node count.

The paper [40] has drawn attention on the potential capability of game theory by taking into account multi-attacker collusion as a novel improvement that can demonstrate the range of random actions of node declination, node attacks, node collaboration and node reporting which may represent strategic profiling of several nodes in MANETs. The proposed framework has been drafted to be a virtual competition that is plotted with predictable strategies which should be adopted by malicious node for attacking and regular node for updating by employing Perfect Bayesian Equilibrium (PBE). The simulation results have shown improved accuracy to capture malicious nodes and their behavior in each round plus the strategy adopted for escaping to a new region. The paper has tried to identify several tasks related to MANET security that are computationally challenging by making use of game theory for analyzing the behavioral pattern of the nodes in the network. Further, the system has the ability to demonstrate the underlying principle of the adopted behavior of nodes when regular and malicious nodes are taken into consideration. As the system adopts PBE to understand the effects of a variety of empirical parameters that are evaluated during the simulation, the framework proposed can be professed to be efficient. Although the results attained show that this system effectively addresses the malicious behavior of nodes in MANETs, the research on security issues of MANETs is still dawning as there is a need of standardizing the protocols and evaluating large-scale networks because of the highly vulnerable wireless adhoc network.

In [41] authors have put forward a secure routing model DTASR – Dual Threshold-based Authentication for Secure Routing that lays emphasis on trust-based authentication and resource-based thresholding schemes for ensuring high resilience against assailants. A safe mitigation strategy has been presented by authors that combat illegitimate access in MANETs. For achieving this objective, a non-cryptographic technique has been employed making use of analytical modeling to attain the highest security level. The system uses probability theory for evaluation of surrounding nodes' reliability for finding out two things, firstly whether adjacent nodes result in more rapid data communication and secondly, whether paths generated by intermediate hops possess high trust factor. After each round of authentication success or failure, the proposed system updates itself after assessing the trust factor. This new trust factor is broadcast for securing remaining routes. In this way, flexibility towards any sort of unauthorized access is discarded and nodes with malicious behavior produce a depreciated trust-factor value. The mechanism utilized by the authors is based on threshold and is thus simple as well as robust due to stable consumption of memory for routing updates. Thus, the technique employed by authors is in compliance with time as well as memory complexity. The proposed model has been found to exhibit an improved communication performance in contrast to the existing routing schemes.In future, further enhancements in security level and comparison with other conventional methods shall be taken up.

In [1] authors have found that current mobile adhoc networks succumb to network partitioning and can be precarious for applications like battlefield communication or crisis management where group members are required to work in teams distributed in the application domain. In these applications, communication among the teams is pivotal for their collaboration. The authors have put forward Autonomous Mobile Mesh Network (AMNET) in this paper. In contrast to the traditional mesh networks, the nodes in AMNETs can follow mesh clients in application domain and then get arranged in the form of a proper network topology for guaranteeing enhanced connectivity in intra as well as inter-group communication. In order to tackle with the frequently changing mobility pattern of clients, a dispersed client tracking solution has been proposed. However, some issues are still there that need to be analyzed for making improvements in AMNETs e.g., utilization of non-overlapping channels, looking for disappeared client, minimization of routing paths, etc. The issues mentioned have been left to be taken in future research.

In [42] authors have presented a new routing scheme for MANETs that is a combination of on-demand routing potential of Ad hoc On-demand Distance Vector (AODV) protocol and the mechanism of scattered topology detection by making use of mobile agents such as ants. This amalgamation offers improved connectivity while slashing the number of route discoveries that have to be made before initiating fresh connections thus eliminating the delays that may arise ahead of setting up a genuine communication. This makes ant-AODV an ideal routing protocol for real time communications for majority of new connections in dynamic networks like MANETs. Nevertheless, endowing the ant agents with intelligence and communication among agents have been left as future work.

In [25] authors have taken up the issues concerning reliability that should be dealt with prior to the use of mobile agents in a wide variety of MANET commercial applications. An algorithm has been proposed by them for estimating how reliable mobile agent systems (MAS) are. These agents have the ability to choose routes dynamically i.e., the task assigned to a mobile agent determines its demand of link capacity. As a result, mobile agents are presupposed to opt a route that is able to satisfy its QoS requisites in context of its link capacity. The future work comprises of fault tolerance in mobile agent systems.

The author in [16] has brought to light several security related issues in mobile adhoc networks that lack proper attention. The paper has also explored counter measures for the issues discussed. The author suggests the requirement of some special security technique since no technique among the existing ones is able to fit all networks seeing that the nodes involved may be any device.

In the paper [43] authors have conducted a survey on the threats to MANET security and their respective solutions. They have concluded that those solutions are not sufficient for the variety of mobile adhoc networks and thus require further research attention.

Authors in [44] have put forward a review of intrusion detection techniques in MANETs and wireless sensor networks (WSN). They have exhibited various security issues in both the networks and the adaptive system proposed by them has been found to produce poor results when encountered by high level of mobility, therefore further improvements need to be made.

In [45] the authors have presented their research work on the threats to MANETs and their solutions by making use of AODV and secure AODV. The susceptibility of the two protocols has been explored when exposed to various risks. Furthermore, directions for future research have also been given like bandwidth allocation in limited resources at the time of resource depletion attack, self healing routing and ability to search multi-path routes in MANETs.

The facts collected from the survey of relevant literature have been presented in Table I given below.

## CHALLENGES

The literature survey draws attention on the difference between wired networks and wireless adhoc networks. Since it is an entirely new architecture, it leads to several challenges. The different researchers have highlighted many challenges and that need proper attention for smooth functioning and to deliver quality of service by MANETs [16] [43] [45]. Various extensive research work conducted in the past shows that mobile adhoc network is girdled with various type of issues e.g. dynamic topologies, inefficient routing policies, unwanted energy depletion, security, etc. These are illustrated as follows:

**1)Infrastructureless:** There is absence of fixed infrastructure, special hardware and centralized servers in MANETs. This restrains implementation of hierarchical host associations. Thus, the nodes support open relationship where nodes operate both as hosts and routers. In this way, their role in the adhoc network is assumed to be collaborative and not reliant that means dependence of security solutions on cooperative rather than centralized schemes.

**2) Quality of Service:** This factor is an assurance given by network for providing quality performance that can be determined by various parameters like bandwidth, packet-

Table I: Review of Previous Work

| Author | Contribution | Result Obtained | Limitations |
|---|---|---|---|
| (Farmer *et al*., 1996)[37] | • Discussed the issues and security requirements in mobile agents<br>• Developed a set of security requirements for mobile agents systems | •Examined the use of mobile agents in several ways while identifying the security issues that must be tackled by security infrastructure | •Investing substantially in mobile agent system needs prospective analysis directed towards mobile agents specifically |
| (Shivanajay *et al*., 2002)[42] | •Proposed a hybrid routing protocol for mobile adhoc networks bringing together the features of AODV protocol and distribution topology discovery technique | •Reduced number of route discoveries before initiating a new connection thus ensuring high connectivity, decreased end-to-end delay<br>•Suitable for real time multimedia/ data communication in extremely dynamic networks | •Extra processing of the ant messages which increase overhead taking up network capacity |
| (Hijazi *et al*., 2005)[36] | •Examined the employability of mobile agents against principal security issues in wireless adhoc networks | •Ideally and feasibly adoptable based solution based on mobile agent for intrusion detection systems in wireless adhoc networks<br>•Analyzed and provided comparison of the present intrusion detection systems based on mobile agents in wireless adhoc networks | •Incorporating mobile agents and deploying them eminently should be done for fulfilment of wireless adhoc networks intrusion detection system constraints<br>•A novel architecture needs to be implemented that is suitable for wireless adhoc networks while offering benefits of both mobile agents and intrusion detection designs |
| (Djenouri *et al*., 2005)[43] | •Put forward discussion on various security issues plus the solutions proposed for them | •Provided review on security of wireless sensor networks(WSN)<br>•Demonstrated in particular several attacks on routing protocols while categorizing the various techniques for their mitigation | •New mechanisms need to be designed that utilize the distinctive character of WSNs |
| (Sun Bo *et al*., 2007)[44] | •Analyzed the intrusion detection mechanism in wireless sensor and mobile adhoc networks | •Focussed on intrusion detection capabilities for construction of intrusion detection system | •Failure to detect false alarm v/s abnormal event<br>•Need of a light weight solution to estimate monitoring features of neighbour<br>•Not feasible at deployment time |
| (Chowdary *et al*., 2011)[25] | •Proposed an algorithm for estimating reliability of task route in mobile agent systems (MAS) on the basis of underlying network conditions | •Dynamic selection of routes by agents<br>•Proposed algorithm has been found to be robust enough | •Based on the assumption that MAS is comprised of several independent mobile agent groups operating simultaneously |
| (Shen *et al*., 2014)[1] | •Introduced Autonomous Mobile Mesh Network(AMNET) as a different category of adhoc networks | •Ensures superior connectivity for inter- as well as intra- group communication by their organization into a feasible network topology<br>•Effectively deals with the dynamic nature of the mobility pattern of client and puts forward a technique for the same<br>•Shows robustness against partitioning of network and provides high relay throughput for clients | •Issues like minimization of routing paths, utilization of non-overlapping channels and looking for disappearing client need to be explored in future for enhancing AMNETs |
| (Khan *et al*., 2015)[13] | •Put forward an energy aware bio-inspired optimization approach-ElePSO | •Produces minimum overhead in collision avoidance scheme and reduces the network congestion<br>•Shows better performance than other optimization techniques like ACO or PSO in terms of enhanced network lifetime, minimum collision probability and least data retransmission | •Degradation in overall performance of network caused due to higher energy consumption |

loss probability and jitter. The numerous applications on the internet are heterogenous in nature like live video, file transfer, voice, etc. which challenge the network to deliver the best quality service to its users.

**3)Use of Wireless Links:** The utilization of wireless links in mobile adhoc networks makes it vulnerable to attacks. In contrast to wired networks in which attackers have to get physical access to network cables or have to bypass a number of defence lines at gateways and firewalls, mobile adhoc networks can be attacked from any direction and any node can be targeted. Therefore, all the nodes should be ready to face threats as MANETs do not have a cleared out line-of-defence. Furthermore, MANETs are susceptible because of the reliance of MAC protocols employed in these networks on faithful collaboration in the neighbourhood for ensuring channel access in view of the widely accessible channel.

**4)Scalability:** Scalability has been taken for granted in MANETs. In the present day, pervasive computing is popular and the network can be expanded to millions of nodes. So there arises an issue of carrying out the numerous control messages in such an environment. Also, the extent up to which a mobile adhoc network can be extended is not clear [27].

**5)Routing and Topology Change:** All the nodes in MANETs can move freely at any instant of time. This gives rise to the rapid and random changes in topology. This signifies that specific mobile node tracking in large-scale MANETs is not easy which can be exploited by security threats. This dynamic topology of MANETs makes routing complex with the worst case being the unpredictability of presence of nodes in the same network the next moment.

**6)Bandwidth:** It is a major constraint because interference, fading, multiple access and noise result in less throughput of the mobile adhoc network.

**7)Energy Constraint:** Nodes in MANETs are light weight and small as a result of which their power resources are restricted for ensuring portability. This drawback makes the network vulnerable because it may breakdown when a node is powered off that may become a target for attackers who detach those nodes or make a partition in the network. This kind of attack is referred to as sleep-deprivation torture attack or energy starvation attack [43]. In order to deal with this, crucial system should be designed that optimizes energy in the mobile adhoc network.

**8)Security:** In general, MANETs are susceptible to physical threats in comparison to wired networks. So, there are risks of intrusion, eavesdropping, denial-of-service and spoofing attacks.

**9)Dynamic IP Allocation:** In MANETs, IP addresses are allocated dynamically to the participating nodes. However, when many mobile adhoc networks merge with each other, IP addresses can be duplicated and their resolution is a difficult task. In this way, IP address duplication can easily lead to attacks thereby resulting in impersonation attacks.

**10)Implicitly Assumed Trust among Nodes:** It is presumed by routing protocols in MANETs that the nodes involved are genuine. This assumption permits direct operation of malicious nodes that may cripple the entire network by simply disseminating false information.

**11)Memory and Reduced Processing Speed:** Mobile nodes in MANETs possess poor computation capability and have restricted storage capacity. But complex security remedies particularly cryptographic schemes require higher processing speeds as well as memory for efficient operation. Furthermore, the distribution and management of key is also an important issue that needs to be tackled for deploying these solutions.

## CONCLUSION

To conclude this, all the issues in the MANETs need proper research attention because all those issues are not fully addressed yet. The origin and main application area of MANETs is military services, so the security is the main issue in MANETs. And mobile agents can possibly overcome these issues by proper research. Mobile agents can be utilized to overcome security, routing and bandwidth issue on the fly in the MANETs. Moreover, in depth research for optimization of MANETs is the need of the hour.

## ACKNOWLEDGEMENT

This work was supported by Ministry of Higher Education Malaysia (Kementerian Pendidikan Tinggi) under Research Initiative Grant Scheme number (RIGS16-084-0248)

## REFERENCES

1. Shen, W.L., C.C. Shiuan, K.C. Lin and K.A. Hua, 2014. Autonomous mobile mesh networks IEEE Transactions on Mobile Computing, 13(2): 364-376.
2. Singh, U., B.V.R. Reddy and M.N. Hoda, 2011. GNDA: Detecting good neighbour nodes in adhoc routing protocol, In Emerging Applications of Information Technology (EAIT), 2nd International Conference on, IEEE, pp: 235-238.
3. Pattnaik, P.K. and Rajib Mall, 2014. Fundamentals of Mobile Computing, 2nd ed., PHI Learning Pvt. Ltd., 2014.
4. Asgharian, H. and B. Amirshahi, 2015. Adaptive and distributed TDMA scheduling protocol for mobile ad hoc networks (MANET), 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI),IEEE, November 2015, pp: 938-942.
5. Madhurikkha, S. and R. Sabitha, 2103. Defending against packet dropping attack using DRI and cross checking mechanism in MANET, In Information Communication and Embedded Systems (ICICES), International Conference on, IEEE, February 2013, pp: 260-264.

6. Li, L., B. Feldman and J. Arge, 2004. Self-organizing security scheme for multi-hop wireless access networks, In IEEE Proceedings on Aerospace Conference, 2: 1231-1240.
7. Hoebeke, J., I. Moerman, B. Dhoedt and P. Demeester, 2004. An overview of mobile ad hoc networks: Applications and challenges, Journal-Communications Network, 3(3): 60-66.
8. Khan, B.U.I., R.F. Olanrewaju and M.H. Habaebi, 2013. Malicious behaviour of node and its significant security techniques in MANET-A review. Australian Journal of Basic & Applied Sciences, 7(12): 286-293.
9. Alshbatat, A.I. and L. Dong, 2010. Cross layer design for mobile ad-hoc unmanned aerial vehicle communication networks, In Networking, Sensing and Control (ICNSC), International Conference on, IEEE, April 2010, pp: 331-336.
10. Olanrewaju, R.F., B.U.I. Khan, F. Anwar and A. Shah, 2015. Strategic profiling for behaviour visualization of malicious node in MANETs using Game Theory, Journal of Theoretical and Applied Information Technology, 77(1): 25-43.
11. Agarwal, P., B.S. Yadav and J. Chandra, 2008. Statistical analysis based efficient decentralized intrusion detection scheme for mobile ad hoc networks, In 16th IEEE International Conference on Networks, December 2008, pp: 1-6.
12. Sharma, L. and P. Dimri, 2015. An improved AODV with QoS support in mobile ad-hoc network, In Computing for Sustainable Global Development (INDIACom), 2nd International Conference on, IEEE, March 2015, pp: 2052-2056.
13. Khan, B.U.I., R.F. Olanrewaju, N.B. Ali and A. Shah, 2014. ElePSO: Energy aware elephant swarm optimization for mobile adhoc network, Pensee Journal, 76(5): 88-103.
14. Haque, I.T., 2014. On the overheads of ad hoc routing schemes, IEEE Systems Journal, 9(2): 605-614.
15. Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK - A secure intrusion-detection system for MANETs, IEEE Transactions on Industrial Electronics, 60(3): 1089-1098.
16. Joshi, P., 2011. Security issues in routing protocols in MANETS at network layer, Procedia Computer Science, 3: 954-960.
17. Ahmad, S.S., S. Camtepe and D. Jayalath, 2015. Understanding data flow and security requirements in wireless body area networks for healthcare, In International Conference on E-health Networking, Application & Services (HealthCom), IEEE, October 2015, pp: 621-626.
18. Kavitha, P. and R. Mukesh, 2015. To detect malicious nodes in the mobile ad-hoc networks using soft computing technique, In Electronics and Communication Systems (ICECS), 2nd International Conference on, IEEE, February 2015, pp: 1564-1573.
19. Khan, B.U.I., R.F. Olanrewaju, F. Anwar and A. Shah, 2014. Manifestation and mitigation of node misbehaviour in adhoc networks, Wulfenia Journal, 21(3): 462-470.
20. Khatawkar, S.D. and N. Trivedi, 2015. Detection of gray hole in MANET through cluster analysis, In Computing for Sustainable Global Development (INDIACom), 2nd International Conference on, IEEE, March 2015, pp: 1752-1757.
21. Shaikh, R.A. and Z. . Shaikh, 2005. A security architecture for multihop mobile ad hoc networks with mobile agents, In Pakistan Section Multitopic Conference, Karachi, December 2005, pp: 1-8.
22. Wei, Z., H. Tang, F.R. Yu, M. Wang and P. Mason, 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning, IEEE Transactions on Vehicular Technology, 63(9): 4647-4658.
23. Kapur, R.K. and S.K. Khatri, 2015. Analysis of attacks on routing protocols in MANETs, In Computer Engineering and Applications (ICACEA), International Conference on Advances in, IEEE, March 2015, pp: 791-798.
24. Zuo, Y. and J. Liu, 2015. Mobile agent-based service migration, In Information Technology-New Generations (ITNG), International Conference on, IEEE, April 2015, pp: 88-13.
25. Chowdhury, C. and S. Neogy, 2011. Reliability estimate of mobile agent system for QoS MANET applications, IEEE Proceedings, In Reliability and Maintainability Symposium (RAMS), 2011, pp: 1-6.
26. Lange, D.B. and M. Oshima, 1999. Seven good reasons for mobile agents, Communications of the ACM, 42(3): 88-89.

27. Penttinen, A., 2002. Research on ad hoc networking: Current activity and future directions. Networking Laboratory, Helsinki University of Technology, Finland, 2002.
28. Conti, M. and S. Giordano, 2014. Mobile ad hoc networking: milestones, challenges and new research directions, IEEE Communications Magazine, 52(1): 85-96.
29. Soelistijanto, B. and M. Howarth, 2013. Transfer reliability and congestion control strategies in opportunistic networks: A survey, IEEE Communications Surveys & Tutorials, 16(1).
30. Han, L., 2004. Wireless ad-hoc networks, vol. 8, October 2004.
31. Janaki, R.S., 2014. A survey on stigmergetic control protocols for distributed ad hoc wireless network, International Journal Of Research In Computer Application & Management, 4(8): 24.
32. Bakshi, A., A.K. Sharma and A. Mishra, 2013. Significance of mobile ad-hoc networks (MANETS), International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2(4).
33. Jennings, N. and M. Wooldridge, 1996. Software agents. IEE Review, 42(1): 17-20.
34. Rothermel, K. and M. Schwehm, 1998. Mobile Agents, Encyclopedia for Computer Science and Technology, 40: 155-176.
35. Bieszczad, A., B. Pagurek and T. White, 1998. Mobile agents for network management. Communications Surveys & Tutorials, IEEE, 1(1): 2-9.
36. Hijazi, A. and N. Nasser, 2005. Using mobile agents for intrusion detection in wireless ad hoc networks, In Second IFIP International Conference on Wireless and Optical Communications Networks, March 2005, pp: 362-366.
37. Farmer, W., J.D. Guttman and V. Swarup, 1996. Security for mobile agents: Issues and requirements. Proceedings of the 19th national information systems security conference, 2: 591-597.
38. Patil, A. and S. Sapre, 2014. Intelligent energy efficient routing protocol based on biological agents for MANETS, IJETAE, 4(7).
39. Mourya, A.K. and N. Singhal, 2014. Managing congestion control in mobile ad-hoc network using mobile agents. arXiv preprint arXiv:1401.4844, 2014.
40. Olanrewaju, R.F., B.U.I. Khan, R.N. Mir and B.W. Adebayo, 2015. Behaviour visualization for malicious-attacker node collusion in MANET based on probabilistic approach. American Journal of Computer Science and Engineering, 2(3): 10-19.
41. Khan, B.U.I., R.F. Olanrewaju, A.M. Baba, R.N. Mir and S.A. Lone, 2015. DTASR: Dual threshold-based authentication for secure routing in mobile adhoc network, International Journal of Information Technology & Computer Science (IJITCS), 22(1).
42. Shivanajay, M., C.K. Tham and D. Srinivasan, 2002. A novel routing protocol using mobile agents and reactive route discovery for ad hoc wireless networks, 10th IEEE International Conference on Networks, 2002, pp: 311-316.
43. Djamel, D., L. Khelladi and N. Badache,2005. A survey of security issues in mobile ad hoc and sensor networks, IEEE Communications Surveys& Tutorials, 7(4): 2-28.
44. Bo, S., L. Osborne, Y. Xiao and S. Guizani, 2007. Intrusion detection techniques in mobile ad hoc and wireless sensor networks, In Proceeding of IEEE on Wireless Communication, 14(5): 56-63.
45. Mulert, J.V., I. Welch and W.K.G. Seah, 2012. Security threats and solutions in MANETs: A case study using AODV and SAODV, Journal of Network and Computer Applications, 35(4): 1249-1259.