Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Study of Malicious Activities & Challenges in MANET's

Rahul Dev Sagar

USICT, Guru Gobind Singh Indraprastha University, Delhi, India

Abstract*— *Mobile ad hoc network comprises of a group of wireless nodes that can be set up anywhere and anytime without using any pre-existing network infrastructure. These allow people and devices to seamlessly internetwork in areas lacking any communication infrastructure. The communication between two nodes is peer to peer and the network traffic is usually consistent. While communication between two nodes beyond a single hop maintains a stable route and is remote to remote. Initially, tactical networks were the only communication networking application, which were on the paths of ad hoc paradigm. However with the introduction of new technologies such as Bluetooth, hyperlan etc., the deployment of MANET can be considered beyond military domain. This paper attempts at providing a comprehensive analysis of the same depicting important role of MANET and latest research activity in the area of MANET.

Keywords: MANET; MAC; Routing; Energy Saving; Security; Performance Evaluation.

I. Introduction

A MANET is a peer-to-peer multi-hop mobile wireless network that has neither a fixed infrastructure nor a central server. Each node in a MANET acts as a router, and communicates with each other. A large variety of Mobile ad-hoc network applications have been developed. A considerable amount of research has recently been proposed for replica allocation in a MANET. It can operate without existing infrastructure, supports mobile users, and falls under the general scope of multi-hop wireless networking. Such a networking paradigm originated from the needs in battlefield communications, emergence operations, search and rescue, and disaster relief operations. The two most important operations at the network layer, i.e. data forwarding and routing, are distinct concepts. Data forwarding regulates how packets are taken from one link and put on another. Routing determines which path a data packet should follow from the source node to the destination. The latter essentially provides the former with control input. Ad hoc wireless networks inherit the traditional problem of wireless and mobile communication; we have some various challenges like Battery Backup, Node Mobility, Bandwidth constraint, Routing Protocols, Security problems and transmission quality enhancement.

In this paper we study the security measures that can be included into routing which can keep the node identity safe from the adversary and also provided for routing of packets without much difficulty.

Fig. 1. Ad Hoc Network

Fig. 2. MANET

II. 4G AND ADHOC NETWORKING

The major aspect of 4G Wireless evolution is to provide for a computing environment that can efficiently support users in accomplishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device [1].

In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need. The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the environment, without requiring any major change in the user's behaviour. This new philosophy is the basis of the Ambient Intelligence concept [2].

This view heavily relies on 4G wireless and mobile communications. 4G is all about an integrated, global network, based on an open systems approach. Integrating different types of wireless networks with wire-line backbone network seamlessly and convergence of voice, multimedia and data traffic over a single IP-based core network are the main foci of 4G. With the availability of ultra-high bandwidth of up to 100 Mbps, multimedia services can be supported efficiently; ubiquitous computing is enabled with enhanced system mobility and portability support, and location-based services are all expected.

The following figure illustrates the components within 4G-network architecture.

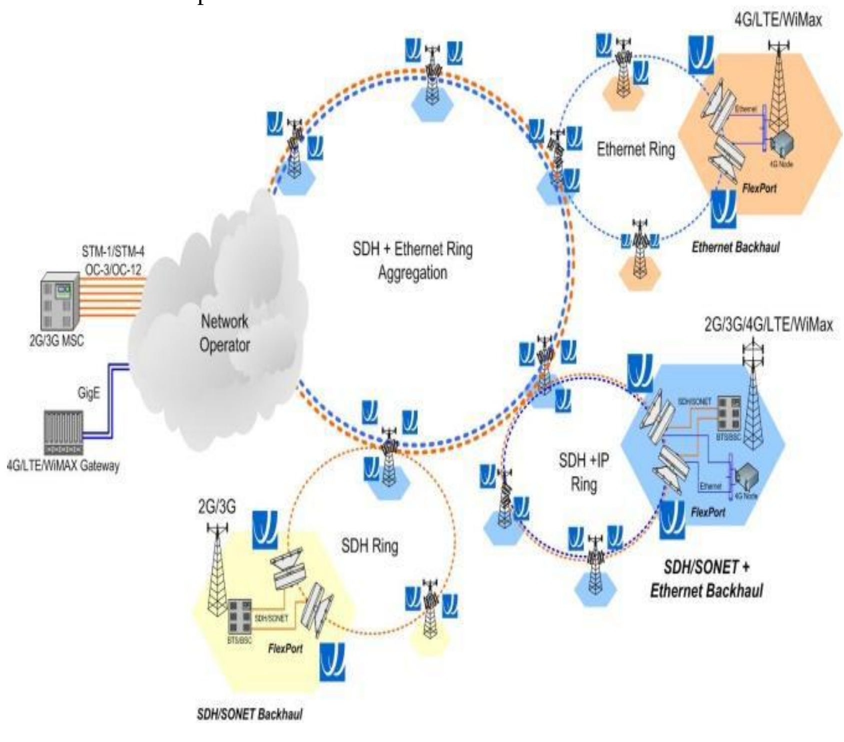

Fig. 3. 4G Network Architecture

There are two levels of integration first is the integration of heterogeneous wireless networks with varying transmission characteristics such as Wireless LAN, WAN, PAN, as well as mobile ad hoc networks. At the second level we find the integration of wireless networks with the fixed network backbone infrastructure, the Internet, and PSTN. Much work remains to enable a seamless integration, for example that can extend IP to support mobile network devices. All IP Networks. 4G starts with the assumption that future networks will be entirely packet-switched, using protocols evolved from those in use in today's Internet [3]. An all IP-based 4G wireless network has intrinsic advantages over its predecessors. IP is compatible with, and independent of, the actual radio access technology, this means that the core 4G network can be designed and evolves Independently from access networks. Using IP based core network also means the immediate tapping of the rich protocol suites and services already available, for example, voice and data convergence, can be supported by using readily available VoIP set of protocols such as MEGACOP, MGCP, SIP, H.323, SCTP, etc. Finally the converged all-IP wireless core networks will be packet based and support packetized voice and multimedia on top of data. This evolution is expected to greatly simplify the network and to reduce costs for maintaining separate networks, for different traffic types. Lower Cost and Higher Efficiency. 4G IP-based systems will be cheaper and more efficient than 3G. Applications.4G systems aim to provide ultra-high transmission speed of up to 100 Mbps, 50 times faster than those in 3G networks. This leap in provided bandwidth will enable high-bandwidth wireless services, allowing users to watch TV, listen to the music, browse Internet, access business programs, and perform real-time video streaming and other multimedia-oriented applications, like E-Commerce, as if sitting in home or office.
4G terminals need to be more intelligent in terms of uses locations and service needs, including recognizing and being adaptive to user's changing geographical positions, as well as offering location-based services [4].

III. MOBILE ADHOC NETWORKS

Adhoc networking capabilities can become very important in delivering overall next generation wireless network functionalities.

IV. ADHOC NETWORK RESERCH

A large body of research has been accumulated to address these specific issues, and constraints. In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain.
The research activities will be grouped, according to a layered approaching to three main areas:
• Enabling technologies;
• Networking;
• Middleware and Applications.
Also several issues (energy management, security and cooperation, quality of service, network simulation) span all areas.

V. ENABLING TECHNOLOGIES

Adhoc networks can be classified on the basis of their coverage area i.e.

- BAN (Body)
- PAN (Personal)
- LAN (Local)
- MAN (Metropolitan)
- WAN (Wide)

Ad-hoc single hop BAN, PAN and LAN wireless technologies are already common on the market [1], these technologies constituting the building blocks for constructing small, multi-hop, ad hoc networks that extend their range over multiple radio hops [5]. For these reasons, BAN, PAN and LAN technologies constitute the Enabling technologies for ad hoc networking.
A body area network is strongly correlated with wearable computers. A wearable computer distributes on the body its components (e.g., head mounted displays, microphones, earphones, etc.), and the BAN provides the connectivity among these devices. The communicating range of a BAN corresponds to the human body range, i.e., 1–2 m. As wiring a body is generally cumbersome, wireless technologies constitute the best solution for interconnecting wearable devices. Personal area networks connect mobile devices carried by users to other mobile and stationary devices. While a BAN is devoted to the interconnection of one-person wearable devices, a PAN is a network in the environment around the persons. PAN communicating range is typically up to 10 m, thus enabling the interconnection of the BANs of persons close to each other, and the interconnection of a BAN with the environment around it. The most promising radios for wide spread PAN deployments are in the 2.4 GHz ISM band. Spread spectrum is typically employed to reduce interference and bandwidth re-use. Wireless LANs (WLANs) have a communication range typical of a single building, or a cluster of buildings, i.e., 100–500 m. A WLAN should satisfy the same requirements typical of any LAN, including high capacity, full connectivity among attached stations, and broadcast capability. However, to meet these objectives, WLANs need to be designed to face some issues specific to the wireless environment, like security on the air, power consumption, mobility, and bandwidth limitation of the air interface [6]. Two different approaches can be followed in the implementation of a WLAN: an infrastructure based approach, or an ad hoc networking one [6]. An infrastructure-based architecture imposes the existence of a centralized controller for each cell, often referred to as Access Point. The Access

Point (AP) is normally connected to the wired network, thus providing the Internet access to mobile devices. In contrast, an ad hoc network is a peer-to-peer network formed by a set of stations within the range of each other, which dynamically configure themselves to set up a temporary network. In the ad hoc configuration, no fixed controller is required, but a controller may be dynamically elected among the stations participating in the communication.

VI. NETWORKING

Most of the major functionalities of network protocols need to be re-designed to cope with dynamic, volatile and peer to peer communication. The aim of the networking protocols is to use the one-hop transmission services provided by the enabling technologies to construct end-to-end (reliable) delivery services, from a sender to one (or more) receiver(s). To establish an end-to-end communication, the sender needs to locate the receiver inside the network. The purpose of a location service is to dynamically map the logical address of the (receiver) device to its current location in the network. Current solutions generally adopted to manage mobile terminals in infrastructure networks are generally inadequate, and new approaches have to be found. Once, a user is located, routing and forwarding algorithms must be provided to route the information through the MANET.

VII. APPLICATIONS

The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the adhoc environment, a great deal of new services can and will be generated for the new environment. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange. Many of these networks consist of highly-dynamic autonomous topology segments. Also, the developing technologies of wearable computing and communications may provide applications for MANET technology [7]. Typical applications include:

Military Battlefield: Adhoc networking would allow the military to take advantage of commonplace network technolog yto maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of adhoc network came from this field.

Commercial Sector: Adhoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld.

Local Level: Adhoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat, small aircraft, mobile adhoc communications will be applied.

Personal Area Network (PAN): PAN is potentially a promising application field of MANET in the future pervasive computing environment. When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for fire/ safety/ rescue operations or other scenarios requiring rapidly deployable communications with survivable, efficient dynamic networking.

VIII. FEATURES

The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly adaptive mobile networking technology to effectively manage multi hop, adhoc network clusters. MANET is advantageous with its several significant features [8] of which some of them are listed below:

1. **Autonomous Terminal**: In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. Besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
2. **Distributed Operation**: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate among themselves and each node acts as a relay as needed, to implement functions security and routing etc.
3. **Multi hop Routing**: The IEEE 802.11 technology is a good platform to implement single-hop adhoc networks. Single-hop is that stations must be within the same transmission area (100-200 meters) to communicate. This limitation can be over come by multi-hop adhoc networking which forwards packets via one or more intermediate nodes [9].
4. **Dynamic Network Topology**: Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes [10]. The nodes in MANET dynamically establish routing among themselves as they move about, forming their own network on the fly. This results in a poor connectivity and in short, network activity bursts.

5. **Fluctuating Link Capacity**: The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.
6. **Lightweight Terminals**: Nodes in MANET are with less CPU processing capability, small memory size and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

IX. CHARACTERISTICS

1. Nodes act as host or router.
2. MANET is capable of multihop routing.
3. Nodes can join or leave the network any time, it make network topology dynamic in nature.
4. In MANET mobile nodes are characterized with less money, power and light weight feature.
5. Intermediate node connectivity.
6. Wireless links are particularly more vulnerable to eavesdropping, spoofing and denial of service (DOS) attacks.
7. It has high-density mobility for number of users.
8. It has robust and low cost network.
9. Wireless connectivity among nodes constrains the bandwidth.

X. CHALLENGES

1. It has limited wireless transmission range.
2. Wireless link characteristic are times varying in nature.
3. It has Packet losses due to error and node mobility in transmission.
4. Mobility induced route changes in routing problem.
5. Broadcast nature of wireless medium has hidden and exposed problems.
6. It has security problem as it is easily snoop.
7. It has frequent network partitions.
8. It has Battery constraint energy efficiency problem [10].

XI. SECURITY ISSUES IN MANETS

MANET is more vulnerable than the wired networks to attacks due to the following major issues [11], [12]:

1. **Lack of centralized management**
   MANET doesn't have any centralized monitoring server. The absence of management control makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large adhoc network. Lack of centralized management impedes trust management for nodes.
2. **Resource availability**
   Resource availability is another issue in MANETs. Providing secure communication in such a dynamic environment as well as protection against specific threats and attacks has led to development of a number of security schemes and architectures.
3. **Scalability**
   Due to mobility of nodes, the topology of adhoc network may change many times. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as a small one.
4. **Cooperation**
   Routing algorithm for MANET usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
5. **Dynamic topology**
   Dynamic topology and continuously changing nodes in the network may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behaviour can be better protected with distributed and adaptive security mechanisms.
6. **Limited Power Supply**
   The nodes in mobile adhoc network need to consider restricted power supply and a node may behave in a selfish manner to save battery power.

XII. CROSS LAYER RESEARCH ISSUES

There are research areas that may affect all layers of an ad hoc system. These include among others energy conservation, security and cooperation, simulation and performance evaluation, and QoS, presented in this section.

1. ENERGY CONSERVATION

Mobile devices rely on batteries for energy. Battery power is finite, and represents one of the greatest constraints in designing algorithms for mobile devices [1, 13, 14]. Projections on progress sin battery technology show that only small improvements in the battery capacity are expected in next future [15]. Under these conditions, it is vital that power utilization be managed efficiently by identifying ways to use less power, preferably with no impact on the applications. Limitation on battery life, and the additional energy requirements for supporting network operations (e.g., routing) inside each node, make the energy conservation one of the main concern in ad hoc networking [16]. The importance of this problem has produced a great deal of research on energy saving in wireless networks in general [17], and ad hoc networks in particular [17,16]. Strategies for power saving have been investigated at several levels of a mobile device including the physical-layer transmissions, the operating system, and the applications [2].

2. NETWORK SECURITY & COOPERATION

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design. Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task [31]. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers_ control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers in applicable. Finally, the security of routing protocols in the MANET dynamic environment is an additional challenge. The self-organizing environment introduces new security issues that are not addressed by the basic security services provided for infrastructure-based networks. Security mechanisms that solely enforce the correctness or integrity of network operations would thus not be sufficient in MANET. A basic requirement for keeping the network operational is to enforce ad hoc nodes contribution to network operations, despite the conflicting tendency (motivated by the energy scarcity) of each node towards selfishness [11, 19].

3. SIMULATION & PERFORMANCE EVALUATION

There are two main approaches in system performance evaluation: the first uses measurements; the second is based on a representation of the system behaviour via a model [18,19]. Measurement techniques are applied to real systems, and thus they can be applied only when a real system, or a prototype of it, is available. Currently, only few measurements studies on real ad hoc test beds can be found in the literature, see e.g., [5, 20]. The Uppsala University APE tested [5] is one of the largest, having run tests with more than thirty nodes. The results from this test bed are very important as they are pointing out problems that were not detected by preceding simulation studies. An important problem, related to the different transmission ranges for 802.11b control and data frames, is the so-called communication gray zones problem [14]. This problem was revealed by a group of researchers at the Uppsala University, while measuring the performance of their own implementation of the AODV routing protocol in an IEEE 802.11b ad hoc network. Observing an unexpected large amount of packets_ losses, mainly during route changes, it was found that increase in packet loss occurred in some specific geographic areas termed called "communication gray zones". In such zones, the packet loss experienced by a station may be extremely high, up to 100%, thus severely affecting the performance of applications associated with a continuous packet flow (e.g., file transfers and multimedia streaming). It was also found that the reason for this phenomenon is that a station inside a gray zone is considered (using the routing information) reachable by a neighbouring station, while actual data communication between the stations is not possible. The same problem was found to affect other routing protocols, such as OLSR. It is important to point out that communication gray zone problem cannot be revealed by commonly used simulation tools (e.g., NS-2, Glomosim), as in these 802.11 models both unicast and broadcast transmissions are performed at 2 Mbps, and hence have the same transmission range.

Constructing a real ad hoc network test bed for a given scenario is typically expensive and remains limited in terms of working scenarios, mobility models, etc. Furthermore, measurements are generally non-repeatable. For these reasons, protocols scalability, sensitiveness to users mobility patterns and speeds are difficult to investigate on a real test sbed. Using a simulation or analytic model, on the other hand, permits the study of system behaviour by varying all its parameters, and considering a large spectrum of network scenarios. Evaluating system performance via a model consists of two steps: (i) defining the system model, and (ii) solving the model using analytical and/or simulative techniques. Analytical methods are often not detailed enough for the ad hoc networks evaluation and in terms of accounting for mobility, in their infancy. On the other hand, simulation modelling is a more standardized, mature, and flexible tool for modelling various protocols and network scenarios, and allows (by running the simulation model) collection and analyses that fully characterize the protocol performance in most cases. A very large number of simulation models have been developed to study ad hoc network architectures and protocols under many network scenarios (number of nodes, mobility rates, etc.). Simulation studies have been extensively applied for instance to compare and contrast large number of routing protocols developed for MANETs, see e.g., [2, 12, 21]. Ref. [13] presents a theoretical framework to compare ad hoc-network routing protocols (in an implementation independent manner) by measuring each protocol's performance relative to a theoretical optimum.

The use of simulation techniques in the performance evaluation of communication networks is a consolidated research area (see [18] and the references herein), however MANET simulation has several open research issues. An in depth discussion of methods and techniques for MANETs simulation can be found in [19]. In the following, we discuss two current topics: (i) models of nodes mobility and (ii) network simulators.

4. QUALITY OF SERVICE

Providing Quality of Service (QoS), other than best effort, is a very complex problem in ANETs, and makes this area a challenging area of future MANET research [22]. Network"s ability to provide QoS depends on the intrinsic characteristics of all the network components, from transmission links to the MAC and network layers [15]. MANET characteristics generally lead to the conclusion that this type of network provides a weak support to QoS. Wireless links have a (relatively) low and highly variable capacity, and high loss rates. Topologies are highly dynamic with frequent links breakages. Random access-based MAC protocols, which are commonly used in this environment (e.g., 802.11b), have no QoS support. Finally, MANET link layers typically run in unlicensed spectrum, making it more difficult to provide strong QoS guarantees in spectrum hard to control [22]. This scenario indicates that, not only hard QoS guarantees will be difficult to achieve in a MANET, but if the nodes are highly mobile even statistical QoS guarantees may be impossible to attain, due to the lack of sufficiently accurate knowledge (both instantaneous and predictive) of the network states [23]. Furthermore, since the quality of the network (in terms of available resources reside in the wireless medium and in the mobile nodes: e.g., buffer and battery state) varies with time, present QoS models for wired networks are insufficient in a self-organizing network, and new MANET QoS model must be defined [21]. Specifically, DiffServ and IntServ (i.e., the Internet QoS models) require accurate link state (e.g., available bandwidth, packet loss rate delay, etc.) and topology information. In [5, 24], an attempt is made to define a MANET QoS model that benefits from the concepts and features of the existing models. The Flexible QoS Model for MANET (FQMM) is based both on IntServ and Diffserv. Specifically, for applications with high priority, per-flow QoS guarantees of IntServ are provided. On the other hand, applications with lower priorities achieve DiffServ perclass differentiation. As FQMM separately applies both IntServ and DiffServ for different priorities, the drawbacks related to IntServ and DiffServ still remain. A more realistic direction for QoS provisioning in ad hoc network is based on an adaptive QoS model: applications must adapt to the time varying resources offered by the network. In [17], the QoS model for a MANET is defined as providing a set of parameters in order to adapt the application to the "quality" of the network. The quality of service provided by the network is not related to any dedicated network layer rather it requires coordinated efforts from all layers. Important QoS components include: QoS MAC, QoS routing, and resource-reservation signalling [25, 26].QoS MAC protocols solve the problems of medium contention, support reliable unicast communications, and provide resource reservation for real-time traffic in a distributed wireless environment [23]. Among numerous MAC protocols and improvements that have been proposed, protocols that can provide QoS guarantees to realtime traffic in a distributed wireless environment include GAMA/PR protocol [21] and Black- Burst (BB) contention mechanism [27]. QoS routing refers to the discovery and maintenance of routes that can satisfy QoS objectives under given resource constraints, while QoS signaling is responsible for actual admission control, scheduling, as well as resource reservation along the route determined by QoS routing, or other routing protocols. Both QoS routing and QoS signaling coordinate with the QoS MAC protocol to deliver the required QoS.

Much research has been done in each of these component areas [2, 17]. INSIGNIA is the first QoS signaling protocol specifically designed for resource reservation in ad hoc environments [7, 18]. It supports in-band signaling by adding a new option field in IP header called INSIGNIA to carry the signaling control information. Like RSVP, the service granularity supported by INSIGNIA is per-flow management. The INSIGNIA module is responsible for establishing, restoring, adapting, and tearing down real-time flows. It includes fast flow reservation, restoration and adaptation algorithms that are specifically designed to deliver adaptive real-time service in MANETs [18]. If the required resource is unavailable, the flow will be degraded to best-effort service. QoS reports are sent to source node periodically to report network topology changes, as well as QoS statistics (loss rate, delay, and throughput). DRSVP [19] is another QoS signaling protocols for MANET based on RSVP.

QoS routing helps establishing the route for successful resource reservation by QoS signaling [16, 27]. This is a difficult task. In order to make optimal routing decision, QoS routing requires constant updates on link state information such as delay, bandwidth, cost, loss rate, and error rate to make policy decision, resulting in large amount of control overhead, which can be prohibitive for bandwidth constrained ad hoc environments. In addition, the dynamic nature of MANETs makes maintaining the precise link state information extremely difficult, if not impossible [27, 25]. Finally, even after resource reservation, QoS still cannot be guaranteed due to the frequent disconnections and topology changes. Several QoS routing algorithms were published recently with a variety of QoS requirements and resource constraints [16,24], for example, CEDAR [29], ticket-based probing [18], Predictive Location- Based QoS Routing [25], Localized QoS, and QoS routing based on bandwidth calculation [16].

XIII. CONCLUSION

In coming years, mobile computing will keep Flourishing and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable. Ad hoc networking is at the canter of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community, as evidenced by the flood of research activities, as well as the almost exponential growth in the Wireless LANs and Bluetooth sectors. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology. From the technical standpoint, as shown in this article, despite the large volume of research activities and rapid progress made in the MANET technologies in the past few years, almost all research areas (from enabling technologies to applications) still harbor many open issues. This is characteristically exemplified by research activities performed on routing protocols. Most work on routing protocols is being performed in the framework of the IETF MANET working group, where four routing protocols are currently under active development. These include two reactive routing protocols, AODV and DSR, and two proactive routing protocols, OLSR and TBRPF. There has been good progress in studying the protocol's behaviour (almost exclusively by simulation), as can be seen in the large conference literature in this area, but the absence of performance data in non-trivial network configurations continues to be a major problem. The perception is that of a large number of competing routing protocols, a lack of WG-wide consensus, and few signs of convergence [21]. To overcome this situation, a discussion is currently ongoing to focalize the activities of the MANET WG towards the design of IETF MANET standard protocol(s) and to split off related long-term research work from IETF. The long-term research work may potentially move to the IETF"s sister organization, the IRTF (Internet Research Task Force) that has recently established a group on „„Ad hoc Network Scaling Research". MANET WG proposes a view of mobile ad hoc networks as an evolution of the Internet. This mainly implies an IP-centric view of the network, and the use of a layered architecture. Current research points out though that this choice may limit developing efficient solutions for MANET. Other promising directions have been identified [28]. The use of the IP protocol has two main advantages: it simplifies MANET interconnection to the Internet, and guarantees the independence from wireless technologies. On the other hand, more efficient and lightweight solutions can be obtained, for example, by implementing routing solutions at lower layers [1, 29]. Furthermore, masking lower Layers characteristics may not to be useful in MANET. The layered paradigm has highly simplified Internet design, however when applied to ad hoc networks, it may result in poor performance as it prevents exploiting important interlayer dependencies in designing efficient ad hoc network functions. For example, from the energy management standpoint, power control and multiple antennas at the link layer are coupled with power control and scheduling at MAC layer and with energy-constrained and delay-constrained routing at network layer [28]. Relaxing the Internet layered architecture, by removing the strict layer boundaries, is an open issue in the MANET evolution. Cross-layer design of MANET architecture and protocols is a promising direction for meeting the emerging application requirements, particularly when energy is a limited resource. From the economic standpoint, the main question to be addressed in the MANET model is the identification of business scenarios that can move MANET"s success beyond the academy and research labs. Currently, apart from specialized areas (battlefield, disaster recovery, etc.), the main business opportunity appears to be in tools (see, e.g., Mesh Networks and SPAN Networks), which let PDAs and/or laptops, set up "self-organizing networks". However, no clear understanding of a MANET killer application(s) has yet emerged. Legacy, content-orientated services and applications enhanced by the self-organizing paradigm could become such an application, as similar to SMS, it would allow to exploit the mobility provided by cellular systems. Users_ benefits gained with the use of the ad hoc technology could make the difference compared to legacy applications (shared whiteboard, chat, file-sharing). Part of bringing the MANET technology to the users is the development of large test beds with direct users_ involvement, as in [19]. In addition to the development of applications and system solutions tailored to the ad hoc paradigm, MANET may offer business opportunities for network service provider, and potentially open the wireless arena to new operators. The lack of infrastructure in MANET is appealing to new commercial systems since it circumvents the need for a large investment to get the network up and running, and the development costs may be scales with network success [28]. Minimum investments, coupled with the emerging tendency (mainly in USA) to deregulate the spectrum environment to create a secondary market, eliminate/reduce the barriers to new operators entering the market to offer new wireless services. However, the MANET potentialities cannot become a reality without an economic model that identifies potential revenues behind MANET-based network services. For example, network services based on the MANET paradigm could be used to efficiently extend the capacity/coverage of Wi-Fi hot spots. It is expected that the bandwidth request in hot spots will increase rapidly, thus requiring higher speed access technologies. With the current 802.11 technology, higher speeds imply a reduction in the coverage area of the Access Point (AP). Spreading in a hot spot a large number of APs to guarantee the coverage is not appealing both from the economic (infrastructure cost) and technical standpoint (APs interference). The ad hoc paradigm can possibly offer an efficient solution to this problem: the APs upgraded with multi-rate high-speed technologies (e.g., 802.11a) achieve the required coverage by exploiting a multi-hop wireless network. While from a technology standpoint, feasible solutions can be designed to apply the MANET technology to extend APs_ coverage; the critical point remains the economic model. Which model could be applied for example in such a scenario to have users cooperating to provide support to the network service provisioning remains a question that typifies the open issues on the way of transitioning MANET results into the business environment. MANET is more vulnerable than the wired networks to attacks due to the following major issues [16], [30]:

ACKNOWLEDGMENT

It is with great sense of gratitude that I express my utmost thanks to Dr. R. Rama Kishore of Department of Information Technology, USICT, GGSIPU, under whose guidance and supervision I had the opportunity to learn and earn knowledge about my seminar and carry out my work. I extend my thanks to him for his valuable suggestions and wholehearted cooperation during the project work. Without his guidance it would not have been possible for me to reach at this level of my project.

REFERENCES

[1] M. Conti, Body, personal, and local wireless ad hoc networks, in: M. Ilyas (Ed.), Handbook of Ad Hoc Networks, CRC Press, New York, 2003 (Chapter 1).

[2] M.G.Zapata, N.Asokan, Securing ad hoc routing protocols, in: Proceedings of ACM Workshop on Wireless Security (WiSe), Atlanta, September 2002.

[3] Wireless World Research Forum (WWRF): http://www.ist-wsi.org.

[4] Y. Bing Lin, Y.R. Huang, A. Pang, I. Chlamtac, All-IP approach for third generation mobile networks, IEEE Network Magazine

[5] M.S. Corson, J.P. Maker, J.H. Cernicione, Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) (1999) 63–70

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci,Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.

[7] Toh, C.K.,“Future Application Scenarios for MANET-Based Intelligent Transportation Systems”, Future generation communication and networking (fgcn 2007), Volume 2, pp 414 – 417, 6-8 Dec. 2007.

[8] K. Weniger, M. Zitterbart, “Mobile adhoc networks – current approaches and future directions,” Network, IEEE, vol 18, Issue 4, pp 6–11, July-Aug 2004.

[9] Rappaport, T.S.; Annamalai, A.; Buehrer, R.M.; Tranter, W.H., “Wireless communications: past events and a future perspective”, IEEE Communications Magazine, Vol. 40, Issue 5, PP 148 – 161, May 2002.

[10] Conti M, Giordano S, "Multihop Adhoc Networking: The Theory", IEEE Communications Magazine, Volume 45, Issue 4, pp 78 - 86, April 2007. 4=10

[11] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.

[12] Website of the IEEE 802.11 WLAN: http://grouper. ieee.org/grups/802/11/main.html.postscript_files.html>.

[13] Andras Farago, Violet Syrotiuk, MERIT: a scalable approach for protocol assessment, in: A.T. Campbell, M. Conti, S. Giordano (Eds.), ACM/Kluwer MONET 8 (5) (October 2003), Special issue on Mobile Ad Hoc Network.

[14] L.Feeney, B.Ahlgren, A.Westerlund, Spontaneous networking: an application-oriented approach to ad hoc networking, IEEE Communications Magazine (2001).

[15] Piyush Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory IT 46 (2) (2000) 388–404.

[16] Web site of the Bluetooth Special Interest Group: http:// www.bluetooth.com/.

[17] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.

[18] Roger Wattenhofer, Li Li, Paramvir Bahl, Yi-Min Wang,Distributed topology control for wireless multihop ad-hoc networks, Proceedings of IEEE INFOCOM, April 2001,pp. 1388–1397.

[19] ETSI Technical Report 101 683, V1.1.1, Broadband Radio Access Networks (BRAN): High Performance Local Area Network (HiperLAN) Type 2; System Overview.

[20] Cecilia Mascolo, Licia Capra, Wolfgang Emmerich, Middleware for mobile computing (a survey), in: Enrico Gregori, Giuseppe Anastasi, Stefano Basagni (Eds.),Advanced Lectures on Networking, Lecture Notes in Computer Science, vol. 2497, Springer, Berlin, 2002.

[21] Jeffrey E. Wieselthier, Gam D. Nguyen, Anthony Ephremides,Energy-efficient broadcast and multicast trees inwireless networks, ACM/Kluwer Mobile Networks andApplications 7 (6) (2002).

[22] J.P. Macker, S. Corson, Mobile ad hoc networks (MANET): routing technology for dynamic, wireless networking, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[23] Cecilia Mascolo, Licia Capra, Wolfgang Emmerich, Middleware for mobile computing (a survey), in: Enrico Gregori, Giuseppe Anastasi, Stefano Basagni (Eds.), Advanced Lectures on Networking, Lecture Notes in Computer Science, vol. 2497, Springer, Berlin, 2002.

[24] Ren_e Meier, Vinny Cahill, STEAM: event-based middleware for wireless ad hoc networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops (ICDCSW_02). .

[25] Dmitri D. Perkins, Herman D. Hughes, A survey on quality of service support in wireless ad hoc networks, Journal of Wireless Communication & Mobile Computing(WCMC), Special Issue on Mobile Ad Hoc Networking: Research, Trends, and Application 2 (5) (2002)503–513.

[26] Klaus Hermann, MESHMdl—a middleware for selforganization in ad hoc networks, in: Proceedings of the IEEE Workshop on Mobile and Distributed Computing (MDC 2003) in conjunction with ICDCS 2003, May 19, 2003.

[27] A.L. Murphy, G.P. Picco, G.-C. Roman, Lime: a middleware for physical and logical mobility, in: Proceedings of the 21st International Conference on Distributed Computing Systems (ICDCS-21), Phoenix, AZ, April 16– 19, 2001, pp. 233–524.

[28] A.J. Goldsmith, S.B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communications 9 (4) (2002) 8–27

[29] C. Mascolo, L. Capra, S. Zachariadis, W. Emmerich, XMIDDLE: a data-sharing middleware for mobile computing, Wireless Personal Communications 21 (2002) 77–103.

[30] C. Bisdikian, An overview of the Bluetooth wireless technology, IEEE Communication Magazine, December 2001.

