MOBILE IP ON MOBILE AD HOC NETWORKS: AN IMPLEMENTATION AND PERFORMANCE EVALUATION USING NS2

Kingsley K. Ofosu, Jamal-Deen Abdulai and Ferdinand A. Katsriku

Department of Computer Science, University of Ghana, Legon-Accra, Ghana

ABSTRACT

Mobile computing devices equipped with transceivers form Mobile Ad Hoc Networks (MANET), when two or more of these devices find themselves within transmission range. MANETs are stand-alone (no existing infrastructure needed), autonomous networks that utilise multi-hop communication to reach nodes out of transmitter range. Unlike infrastructure networks e.g. the Internet with fixed topology, MANETs are dynamic. Despite the heterogeneous nature of these two networks, integrating MANETs with the Internet extends the network coverage area of the Internet, and adds to the application domain of MANETs. One of the many ways of combining MANETs with the Internet, is the use of Mobile Internet Protocol (Mobile IP) alongside a MANET routing protocol, to route packets between the Internet and the MANET, via Gateway agents. In this paper, we evaluate the performance of Mobile IP on MANET in Network Simulator 2 (NS2). We have implemented Mobile IP on Ad hoc On-demand Distance Vector (AODV), Ad hoc On-demand Multiple Distance Vector (AOMDV) and Destination-Sequenced Distance Vector (DSDV) routing protocols, and compared performances based on Throughput, End-to-End Delay (E2ED), Packet Delivery Ratio (PDR) and Normalized Packet Ratio (NPR). The simulation results suggest that, on-demand routing within the MANET better serves Mobile IP on MANETs.

KEYWORDS

Mobile Ad Hoc Network, Mobile IP, AODV, AOMDV & DSDV

1. INTRODUCTION

Communication has shifted from a predominantly wired setup towards an entirely wireless setup, or a merger. Computer networks aid in faster and reliable communications over long distances. The Internet, a network of networks, has become a vital utility in our lives that enable us to communicate around the globe. Mobility as a feature in communication has gained the acceptance of end-users. Therefore, it is not surprising that Mobile Ad hoc Networks (MANETs) have attracted much attention from researchers. *A MANET is an autonomous, infrastructure-less, self-forming and self-repairing data network of mobile devices that support multi-hop communication*. MANET could be used to provide Internet connectivity beyond the reach of fixed or cellular infrastructure [1].

The Mobile Internet Protocol (MIP), which was designed to allow mobile nodes to move inside the fixed Internet without losing connectivity, has been experimented in MANET to provide Internet connectivity. We have implemented three variants of Mobile IP on MANET:

- Mobile IP on Ad Hoc On-demand Distance Vector (AODV)
- Mobile IP on Ad Hoc On-demand Multiple Distance Vector (AOMDV)
- Mobile IP on Destination-Sequenced Distance Vector (DSDV)

and evaluated their performances using Network Simulator 2 (NS2).

DOI:10.5121/acij.2018.9202

2. LITERATURE REVIEW

Not much work has been published concerning providing Internet connectivity for MANETs. A number of publications have suggested corporation between Mobile IP [2] and an ad hoc routing protocol to provide Internet access for MANETs. In "Ad Hoc Networking with Mobile IP" [3], a solution was presented whereby a proactive MANET routing protocol was used with Mobile IP. This solution was not compatible with on-demand routing in MANET. In "MIPMANET – Mobile IP for Mobile Ad Hoc Networks" [4], an on-demand MANET routing protocol (AODV) is used alongside Mobile IP with *foreign agent care-of-addresses*, to connect a MANET to the Internet. Likewise MIPMANET, the Internet draft "Global Connectivity for IPv4 Mobile Ad hoc Networks" (Global4) [5] presented a solution whereby AODV interacts with Mobile IP. However, the foreign agent discovery mechanism is incorporated into AODV.

Other publications have used different gateway discovery methods within the MANET routing protocol instead of Mobile IP. The publication titled "Wireless Multihop Internet Access: Gateway Discovery, Routing and Addressing" [6] discusses how MANET nodes can discover gateways to the Internet, the issue of routing, and addressing in heterogenous environments. The master's thesis "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS2" [7] implemented the Internet draft "Global Connectivity for IPv6 Mobile Ad hoc Networks" [8] also known as Global6 in NS2. The AODV routing protocol was modified to include three different gateway detection mechanisms that were tested using NS2 simulations.

Regarding papers that focused more on performance analysis, [9] and [10] conducted separate performance evaluation of Mobile IP on proactive and reactive MANET routing respectively.
Prior to discussing these papers further and their relation to this paper, we will discuss Mobile Ad hoc Networks and the Mobile IP protocol in Sections 2.1 and 2.2 respectively. We will return to these papers as we discuss related works to this paper in section 2.3.

2.1. Mobile Ad Hoc Networks

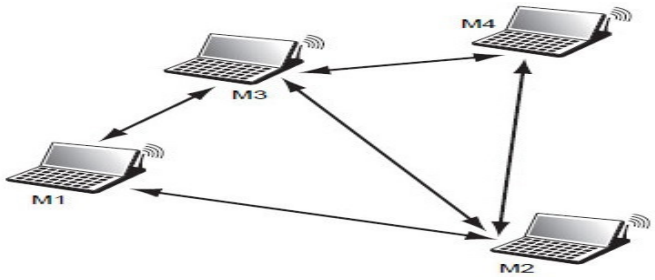


Figure 1. Mobile Ad Hoc Network.

[11] defines a MANET as a self-organizing network of various devices responsible for seamless communication. Although this definition is generally acceptable, it does not reflect some key features of MANET namely: non-dependence on pre-existing network infrastructure, and decentralized management.

A better definition of a MANET would be "an autonomous, infrastructure-less, self-configuring, and self-healing system of mobile nodes connected by 1wireless links" [12]. We extend this further to define a MANET as *an autonomous, infrastructure-less, self-forming and self-repairing network of movable devices that supports multihop communication*. Multihop communication is a critical feature utilized in MANET because nodes are tiny, and battery powered and so cannot transmit over long distances. As such, each participating node also serves as a router to be used as an intermediary node or hop in passing on datagram between source and destination, when destination is not within transmission range of source node.

Traditional networks otherwise known as fixed-infrastructure networks differ from MANET in many ways. Unlike traditional networks that have fixed topology, MANET nodes are free to move in any direction resulting in a dynamic topology which makes designing MANET routing protocols a difficult task. Traditional networks are predominantly wired but MANET communications are strictly wireless. The wireless nature of MANET makes them more susceptible to interference and attenuation resulting in frequent network breaks. MANET nodes are energy constrained as they are powered by tiny batteries, but traditional network nodes usually have a constant energy supply source. MANET are self-organized, self-repairing, and autonomous but traditional networks are setup and managed by networks administrators.

2.1.1. MANET Application Areas

Disaster Recovery: Perhaps the most important application of MANET is during disaster recovery. In disaster situations, there is destruction of infrastructure which may include network infrastructure. In such scenarios, MANET are used to transmit messages and to assist the rescue efforts. [13] presents a survey of the use of MANET in disaster scenarios.

Sensor Networks: A sensor network, also referred to as Wireless Sensor Network (WSN) is a network of tiny sensor nodes with a wireless ad-hoc communication module attached. They sense and record specified environmental phenomenon, and transmit the data using multihop techniques to a central point known as the sink. [14] presents a survey of recent WSN applications.

Military Applications: Initial use of MANET was for military applications. The Defence Advanced Research Projects Agency (DARPA) of the U.S. Department of Defence conceived the use of MANET and researched into it as early as 1973 [15]. Armed forces and equipment are deployed in remote areas without pre-existing network infrastructure. Obviously, installing a cellular system with transmission towers in the battlefield is not practical. In such scenarios, a more practical solution would be to install transmitters with relatively low power in the soldiers backpacks such that, any soldier can only communicate directly with a few other soldiers however, transceivers should be designed in a way that they can forward messages over multiple hops without significant delays [16], thus forming an ad hoc network. The Near Term Digital Radio (NTDR) [17] was one of the earliest ad hoc based systems used by the U.S military. [18] presents a survey of military applications in Wireless Sensor Networks.

Entertainment: In recent times, multiplayer computer games have adopted the use of ad hoc networks whereby as many as eight users could be linked together and compete against each other. Also, robotic pets have been designed to utilize MANET in accepting commands from owners and to entertain their owners.

2.1.2. Routing

Commuters are often faced with the problem of routing on their journeys. When moving from home to a chosen destination, they decide which course or way to journey on. They consider distance, reliability, security, and perhaps traffic levels when choosing a course to travel from source to destination. This essentially describes the idea of routing in computer networking. In computer networking, routing is a generic term for the movement of data from a node (source) to another node (destination). Routing occurs at layer 3 of the *TCP/IP* model which resembles the MANET protocol presented in *Figure 2* below. Routing could be reduced to two fundamental tasks, *route discovery* and *packet switching*. Prior to deciding which routes to take on a journey, we must first equip ourselves with the existing paths that link our source to destination and their properties or metrics. This task is the route discovery phase of routing. After routes are discovered, an optimum route is chosen along which to transport data from the source to destination and then follows packet switching.

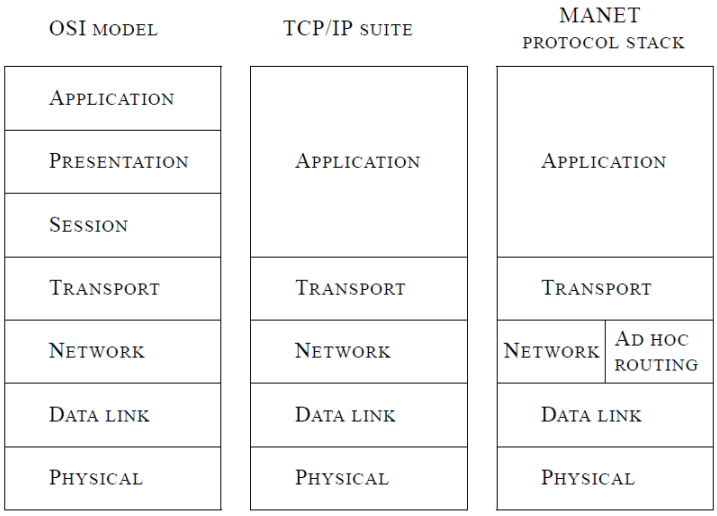


Figure 2. *The OSI Model, TCP/IP Suite* and *MANET protocol stack* [7]

Route Discovery

In MANET, nodes share information on existing routes and their metrics. This could be a scheduled update as defined by the routing protocol or at the request of a node. Routing protocols use metrics such as *hop-count* to decide an optimal route for forwarding data. This information is stored in a conceptual tabular form known as the *routing table*. A typical routing table of a MANET routing protocol will have columns describing source, destination, number of hops, the next hop, and perhaps a sequence number. The nature of routing table data is determined by the type of routing algorithm employed. How route discovery is handled categorizes routing protocols into proactive versus reactive (on-demand). We will discuss routing algorithms and MANET routing protocols in sections 2.3.3 and 2.4 respectively.

Packet Switching

In MANET, each node is a router and so, switching in MANET slightly differs from switching in a fixed-infrastructure network of non-router nodes and routers. In a fixed-infrastructure network, a node sends its data to the router using its Media Access Control (MAC) address and provides in the packet, an IP address of the intended destination. The router then decides a path for the packet or drops the packet, if no path to destination exists. During this process, the MAC address headers of the packet changes, but the IP address of source to destination remain unchanged. A MANET node may either decide a complete path to destination and add the information to the packet before sending to the next hop or may just provide a destination address and send the packet to the next-hop associated with the desired destination in its routing table.

Routing Algorithms vs Routing Protocols

It is a usual occurrence that scholars interchangeably use *routing algorithms* and *routing protocols* during academic writing, which by inference would have the same meaning however, routing algorithms differ from routing protocols. Like a traffic officer directing motorist and pedestrians at an intersection, a routing algorithm is a formula that resides inside a router and determines the path datagrams take. Routing algorithms only operate at the packet switching level whereas routing protocols define the rules of route discovery, route maintenance, and packet switching. It is the routing protocol that provides the initial data that a routing algorithm uses in its calculations and dynamically decides which routing algorithm(s) is/are used in a router. Famous amongst routing algorithms are the Dijkstra Shortest Path First (SPF) [19] [20] and the Bellman-Ford algorithms [21]. Bellman-ford's algorithm successfully deals with negative weights

whiles Dijkstra's does not. Routing algorithms can be grouped into *link-state* versus *distance vector* algorithms. In link-state based routing, nodes keep data in their routing tables to give them a view of the entire network, whereas distance vector algorithms are only interested in immediate neighbours' data. Dijkstra's Shortest Path First and Bellman-Ford's algorithms are link state based whereas a variant of Bellman-Ford's algorithm known as Distributed Bellman-Ford (DBF) is used in distance vector routing. DBF algorithms store very few information on links that are not directly connected to the node [22]. See [23] for a further discussion on routing algorithms.

2.1.3. Manet Routing Protocols

Initially, MANET routing protocols were proactive. They store and update periodically, information on existing paths to all possible destinations for data delivery. Proactive protocols are quicker in choosing routes for data delivery, however, they do not easily converge [22]. E.g., Destination-Sequenced Distance Vector (DSDV) [24]. Reactive or On-demand protocols unlike the proactive protocols, do not anticipate routes between nodes. Nodes discover routes only when there is data to transmit. These protocols only maintain a node neighbour list necessary for route solicitation. E.g. Ad hoc On-demand Distance Vector (AODV) [25].

Destination-Sequenced Distance Vector (DSDV)

DSDV is based on a distance-vector algorithm and guarantees a loop-free route, unlike earlier distance vector based routing protocols by introducing sequence numbers [24]. Nodes maintain a routing table of all destinations with information on the next-hop to the destination, the number of hops, and destination sequence number.

Periodically, a node shares its route table information with neighbouring nodes known as *route updates*. Attached to each update is a sequence number. An odd sequence number indicates an unreachable destination, whereas an even sequence number indicates a reachable destination. The greater the sequence number, the fresher the update.

It is possible to have different updates to the same destination with the same sequence number. In such scenarios, nodes prefer the route with a lesser number of hops to the destination.

Ad Hoc On-demand Distance Vector (AODV)

AODV is a reactive protocol that is based on the distance vector algorithm. AODV discover and maintain routes between two nodes only when they wish to communicate or when a node serves as an intermediate node for forwarding data to help maintain connectivity between two other nodes. Loop-free routes are guaranteed with the use of sequence numbers. The higher the sequence number the fresher the route, and so nodes update their route tables accordingly. Each node maintains a routing table containing a single path entry for each destination it is communicating with [7]. According to [25], AODV's primary objectives are:

- To broadcast discovery packets only when necessary
- To distinguish between local connectivity management (neighbourhood detection) and general topology maintenance
- To disseminate information about changes in local connectivity to those neighbouring mobile nodes that are likely to need the information.

AODV achieves these objectives by using four basic mechanisms: *path discovery*, *route table management*, *path maintenance* and *local connectivity management*.

***Path Discovery*:** AODV performs path discovery using broadcasting technique. Each node maintains two counters: the *sequence number*, and the *broadcast ID*. When a node wishes to communicate with another node, it first checks to see if there is a route entry in its table. In the case where there is no recorded route to reach destination, it starts the process of path discovery.

The source node broadcasts a packet known as the *route request (RREQ)* packet to its neighbours. The route request message contains the address of the sending node, the sequence number as generated by the sending node, the broadcast ID, the destination address, the last known destination sequence number and lastly, the number of hops to destination. The source sequence number together with the broadcast ID uniquely identifies a RREQ. A node upon receiving a RREQ checks its routing table for a path to the specified destination. It checks its own sequence number to the destination and compares with the destination sequence, as specified by the source in the RREQ. If its own destination sequence is greater than that specified in the RREQ, it replies with a *route reply (RREP)* message. Otherwise, it increases the hop count of the RREQ message and rebroadcasts to its neighbours. Nodes usually avoid rebroadcasting the same RREQ message received from different neighbours.

As the RREQ traverse the network, a path known as the *reverse route* is formed. Each intermediate node sets a *reverse pointer* to the neighbour from which the RREQ message was received, before it rebroadcasts the RREQ in the case where it cannot reply the RREQ. The reverse pointer is maintained for a period which is long enough for the RREQ to traverse the network (about 3000 msec) [25]. This period is known as the *reverse path expiration time*. The intermediate node also keeps track of the destination address, source address, broadcast ID and the source sequence number together with the reverse path expiration time. This information will be used to construct the reverse path, which is setup to transmit the eventual RREP, and to construct the *forward path* which is setup during transmission of the RREP [25].

If the destination as specified in the RREQ remains connected to the ad-hoc network, the RREQ will reach a node that has a current path to the destination, if not the node itself. When this happens, a RREP is sent to the source using the reverse route. The RREQ contains the source address, destination address, destination sequence number, hop count to destination and the lifetime. As the RREP travels to the source, each intermediate node now sets a counter to the node from which the RREP was received, before forwarding the RREP. It also updates its timeout information on route entries of source, destination, and adopts the latest sequence numbers. This leads to a forward path setup, that the source will use to reach the intended destination after receiving the RREP. Upon receiving the first RREP, the source node can begin data transmission. If a better route is learnt from subsequent RREPs, thus a less hop count or higher sequenced route, it updates its table and continues data transmission along that route [4].

***Route Table Management*:** Each node running AODV manages a logical tabular information on routes known as the route table. Each route entry in the table contains the destination address, next-hop address, number of hops, sequence number for the destination, active neighbours and the expiration time for the route.

***Path Maintenance*:** When a route is used to transmit data, AODV resets the route's expiration time. Route table entries are used to maintain active neighbours, and active routes. A node is considered active along a route to a destination, if it forwards or generates at least one packet, before the timer runs out. Likewise, a route is marked active if it is used at least one time, by an active neighbour, before the route timer runs out. Inactive routes and neighbours are deleted from the routing table when their timers' runout. Also, when a node detects a broken link, it increases its sequence number for the destination and sets the hops-to-destination field to infinity, before broadcasting the route to its active neighbours. This type of broadcast message is known as an *unsolicited RREP*.

Local Connectivity Management: AODV detects neighbouring nodes through *hello* messages or other forms of broadcast messages received from other nodes. Hello messages are special unsolicited RREP that a node broadcasts after a period (*hello interval*), whereby no messages were sent to all active neighbours. This ensures that nodes update local connectivity even when there is no data exchange. It contains the sending node's address and its current sequence number thus; the node does not increase its sequence number when broadcasting a hello message. As this

message is intended for local neighbours only, it is tagged with a *Time-to-Live* (TTL) value of 1. This prevents all nodes that receive the hello message from rebroadcasting, after updating their local connectivity information. The use of hello messages in AODV can be debated, since they defeat the reactive nature of the protocol. The hello messages adds a significant overhead to AODV however, compared to classical routing protocols like distance vector, AODV has greatly reduced the number of routing messages in the network [26]. As mentioned earlier, a node may learn of new neighbours when it receives a broadcast message other than a hello message from them. When a broadcast message is received from a node that is not already included in its neighbours list, the node is considered a new neighbour and its address with its sequence number is added to the neighbours list.

Ad Hoc On-Demand Multiple Distance Vector (AOMDV)

AOMDV is an extension of AODV routing protocol. The primary goal of AOMDV is to provide efficient fault tolerance by ensuring faster and efficient recovery from route failures in dynamic networks [27]. This goal is met by computing multiple *loop-free* and *link-disjoint* paths during each route discovery process (multi-to-one), instead of a single path during each route discovery process (one-to-one) as seen in AODV. Since the multiple paths computed are disjoint in terms of intermediate nodes, it is less probable that they fail at a go. Alternate paths are tested when the primary path fails. It is only when all paths to the destination are broken that a new route discovery process is initiated. This ensures that AOMDV further reduces the routing overhead in AODV.

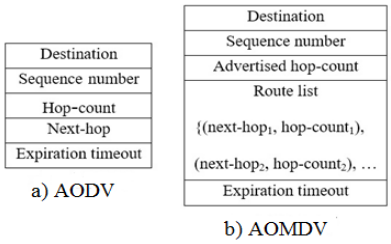


Figure 3. Routing Table Entries for AODV and AOMDV

In AOMDV, *advertised hop-count* replaces the *hop-count* information in AODV route advertisements as shown in *Figure 3*. The advertised hop-count at an intermediate node 'a', is the maximum hop-count of the multiple paths from 'a' to the destination. Also, a *route list* replaces the *next-hop* details in AODV. The route list defines multiple next-hop leading to the same destination and their associated hop-counts, all having the same sequence number. There are two major components of AOMDV: computing multiple loop-free paths and finding link-disjoint paths. See [27] and [28] for further discussions on the components of AOMDV and a performance analysis.

2.2. Mobile IP

Mobile IP works by allowing the Mobile Node (MN) to maintain two IP addresses: the *home address* and the *Care-of-Address (CoA)* [2]. The home address is static and binds MN to a known network called the *Home Network (HN)*. This address is used by transport and application layer protocols to maintain connectivity with MN. On the other hand, the CoA is a dynamic address that MN obtains as it moves outside HN into an unknown network termed as a *Foreign Network (FN)*. The CoA reflects the physical location of MN outside of HN. When MN moves from the HN into FN, it sends the CoA obtained, to the *Home Agent (HA)* on its HN via a similar agent on FN known as *Foreign Agent (FA)*. This message prompts HA to receive packets destined for MN and arriving at HN on behalf of MN, and then tunnels the packets to the CoA. MN repeats this procedure each time MN obtains a new CoA. There are three building blocks of Mobile IP: *agent discovery*, *registration* and *datagram delivery*.

2.2.1. Agent Discovery

This process is an extension of the router advertisement procedure, as specified in the *Internet Control Message Protocol (ICMP)* router discovery messages in *RFC 1256* [29]. Specifically, the only difference is that an agent advertisement has one or more CoAs made available by FA.
[2] explains that an agent advertisement does the following:

- Allows the detection of mobility agents
- Lists the available CoA
- Informs MN of the services offered by FA e.g. alternative encapsulation techniques
- Aids MN to determine its network address and the status of the link to the Internet
- Helps MN to determine whether the agent is a Home Agent, Foreign Agent or both, and therefore whether it is inside HN or FN.

Agents broadcast advertisements periodically; once a second or once every few seconds. However, an MN may solicit for an agent advertisement regardless of this schedule.

2.2.2. Registration

When MN has a new CoA, it must inform HA to render its services to MN. This procedure is known as registration [1]. MN sends a registration request containing:

- Current CoA
- How long MN intends to use the CoA i.e. *Time-to-Live (TTL)*
- Parameters and flags that specify how HA should forward packets
- Special services that MN requests of HA.

When HA receives the registration request, it then authenticates MN and then decides whether to accept or reject, depending on the outcome of the authentication process. HA sends a reply to MN via FA. If HA accepts the request, it maintains in its cache the home address, CoA and the TTL that MN specified in the request. This trio is known as a *binding information*; therefore, registration request is sometimes referred to as a *binding update*. Although the FA remains passive in this process, it maintains a visitors list of each MN that successfully registers with HA through it.

2.2.3. Datagram Delivery

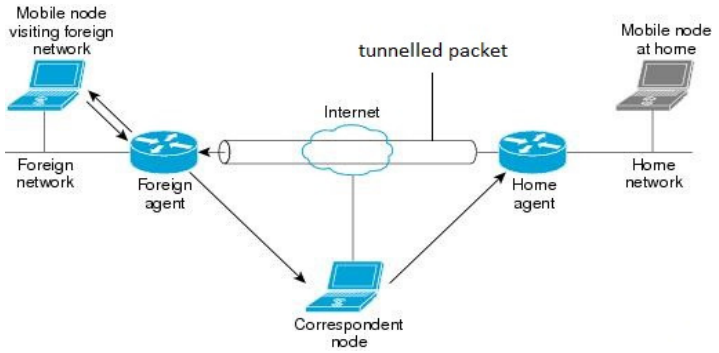


Figure 4. Mobile IP architecture.

As illustrated in *Figure 4* above, the Corresponding Node (CN) transmits packets destined for MN towards HN through standard IP routing. When the packets reach HN, the HA accepts these packets as though it is MN. HA then encapsulates the packet with the CoA as the new destination and forwards the packets to MN. This process is known as *tunnelling*. Two tunnelling protocols often used are *IP within IP* [30] and *minimal IP within IP* [31]. HA continues to receive packets on behalf of MN until TTL runs out. If MN wishes to continue this service, it must register again.

2.3. Related Works

In this section, we discuss some closely related works to this paper as we build up the motivation for this study.

In [3], a proposal for connecting MANET to the Internet using Mobile IP is presented, in which a modified Routing Information Protocol (RIP) like DSDV was used in routing packets within the MANET. In this proposal, a single routing table is used and shared by Mobile IP and the MANET routing protocol, to reduce the management tasks involved in maintaining separate routing tables for Mobile IP and the MANET protocol. Therefore, a route manager is introduced to coordinate route table management between Mobile IP and the modified RIP on the shared routing table. With this, neither Mobile IP or the modified RIP could modify the routing table directly. Route manipulation requests are sent to the route manager which then acts on behalf of the protocols. Although this proposal was successful in providing Internet access to the MANET, it was more proactive and did not support reactive MANET protocols; since it relied on the periodic control messages of the MANET routing protocol to propagate agent advertisements.

To fill the gap, [4] presented a master thesis that detailed the use of Mobile IP on a reactive MANET routing protocol. The authors implemented Mobile IP on AODV in NS2 and then performed some simulations to validate their study. In this proposal, the authors used Mobile IP with Foreign Agent care-of-addresses to reach Mobile Nodes from the Internet. Packets were exchanged between Home Agent and the Mobile Node via *reverse tunnelling* to minimize the requirements on AODV. A novel Internetworking unit was introduced between Mobile IP and AODV to ensure that no modifications be made to Mobile IP outside the MANET. The emphasis of the thesis was not on performance evaluation; therefore, the simulations were not quite extensive.
Also, the Internet draft "Global Connectivity for IPv4 Mobile Ad Hoc Networks" [5] sometimes referred to as Global4, presented a solution which involves the use of Mobile IP with foreign agent care-of-addresses and AODV; just as was done in MIPMANET. However, foreign agent discovery was made a part of AODV, while mobile node registrations with the foreign agent via Mobile IP is maintained.

In the paper titled "Wireless Multihop Internet Access: Gateway Discovery, Routing and Addressing" [6], an alternative approach to providing Internet Access for MANETs is described. In this approach, Mobile IP is eliminated. The use of specific routers that serve as gateways resolve the heterogeneity between the fixed Internet and the MANET. Although the solution looks promising, it was based on IPv6 networks which has not gained popularity over IPv4 networks.

Again, the master's thesis "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS2" [7] implemented the Internet draft "Global Connectivity for IPv6 Mobile Ad hoc Networks" [8] also known as Global6 in NS2. Global6 is an enhancement on Global4; however, Mobile IP services are not used. The AODV routing protocol was modified to include three different gateway detection mechanisms that were tested using NS2 simulations. The gateway detection mechanisms were classified as follows: proactive, reactive and hybrid. The results from simulations showed no significant difference in packet delivery ratio between the three gateway discovery mechanisms. However, the proactive and hybrid mechanisms performed slightly better than the reactive mechanism regarding average end-to-end delay.

With regards to measuring performance of Mobile IP on MANET, [9] evaluated the performance of Mobile IP on a proactive MANET protocol, DSDV. They created simulation scenarios involving a Home Agent, three Routers, four Foreign Agents, a Corresponding Node, and a varying number of Mobile Nodes at varying speeds. Number of nodes were varied to test the robustness of the solution as traffic increases within the simulation space. This was done to rightly model the real Internet world, with its exponential increase in number of mobile devices.

They evaluated performance of Mobile IP based on: received packets, lost packets, throughput and End-to-End Delay (E2ED).

Also, [10] performed simulations in NS2 to evaluate the performance of Mobile IP on AODV. They used a single Home Agent and one Foreign Agent on a 670 ×670 rectangular field with a few Mobile Nodes. Performance metrics used were: throughput, delay and packet overhead. Although the methodology was convincing, the simulation setup was poorly described.

In our paper, we take these works further as we present on the same simulation platform, scenarios to evaluate the performance of Mobile IP on both reactive and proactive MANET routing on IPv4 networks. Our choice of solution involving corporation between Mobile IP and a MANET routing protocol over methods involving IPv6 is mainly because IPv4 as of now is still widely used over IPv6.

We evaluate the performance of Mobile IP on MANET by performing simulations in Network Simulator 2 (NS2). Likewise in [9], we vary number of nodes in our simulation scenarios to account for increasing traffic within the network.

3. METHODOLOGY

As mentioned earlier, we modelled a Mobile Ad Hoc Network using Network Simulator 2 software. Due to the overwhelming dynamism and cost involved in running a live experiment, we chose a computer simulation model specifically using NS2, which has a widely accepted error margin within the networking research community.

3.1. Simulation Scenario

We used a square flat surface of dimension 670m×670m with a simulation time of 200sec as seen in Figure 3. We modelled the fixed Internet using a Home Agent and four Foreign Agents, all with a transmission range of 100m. We placed a gap of 5m between any two adjacent agents. The gap was to ensure that Mobile Nodes decide between Foreign Agents quickly. We simulate up to 175 Mobile Nodes. For each number of Mobile Nodes selected, we performed at least 10 different simulation runs and averaged our results.

Table 1. Simulation Parameters.

Parameter	Value
Movement model	Random waypoint
Traffic type	CBR
MAC layer	802.11
Transmitter range	~100m
Bandwidth	5Mbps
Simulation time	200sec
Simulation field	670m×670m
Number of foreign agents	4
Packet rate	1Mbps
Pause time	0
Maximum speed	5m/s

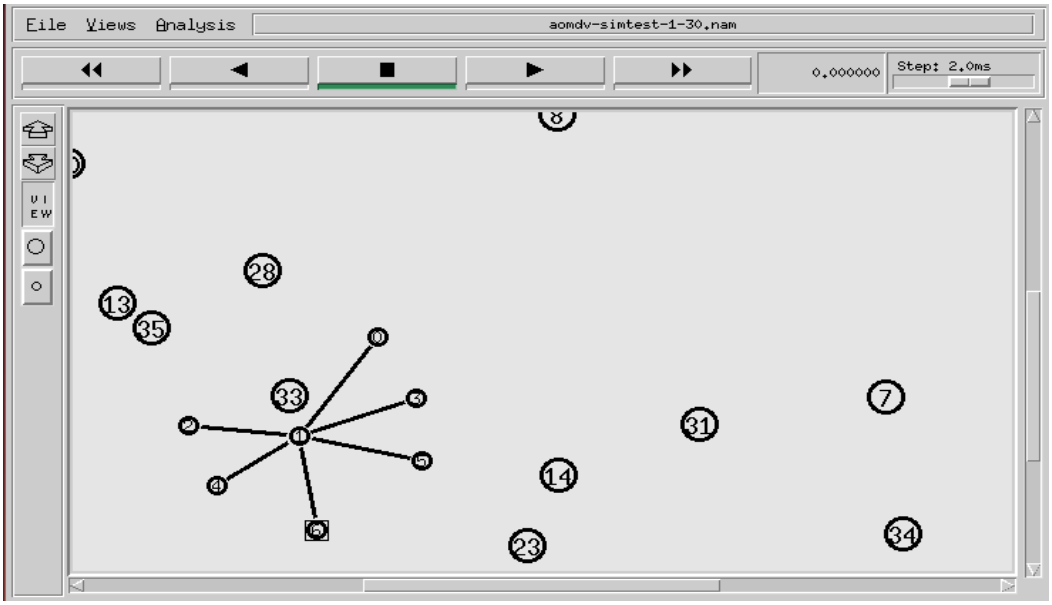


Figure 5. Wired cum wireless scenario.

4. RESULTS AND DISCUSSION

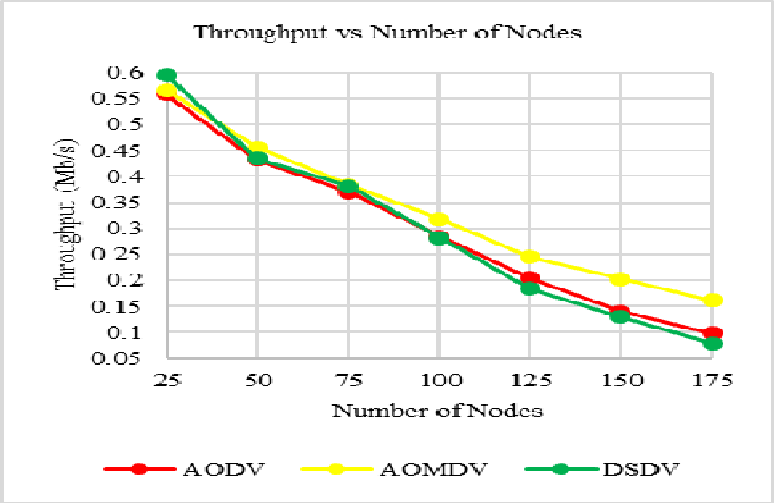


Figure 6. Throughput in Mb/s.

Figure 6 above shows the network throughput as recorded in our simulations. Throughput is a measure of the actual data that can be sent across a channel per unit time. Throughput is usually lesser than channel bandwidth because, channel bandwidth is just a theoretical estimation of how much data could be sent across a channel per unit time. In measuring the network throughput, we excluded control packets and focused on the CBR data packets only. This is sometimes referred to as *Goodput*. Our results show that, throughput decreases as number of nodes increase. AOMDV had the best throughput performance whereas DSDV had the worst, as number of nodes increased. The observed difference in performance is because, AOMDV sends fewer control messages to nodes than AODV and DSDV; therefore, the channel is less occupied and data packets can be transmitted with ease.

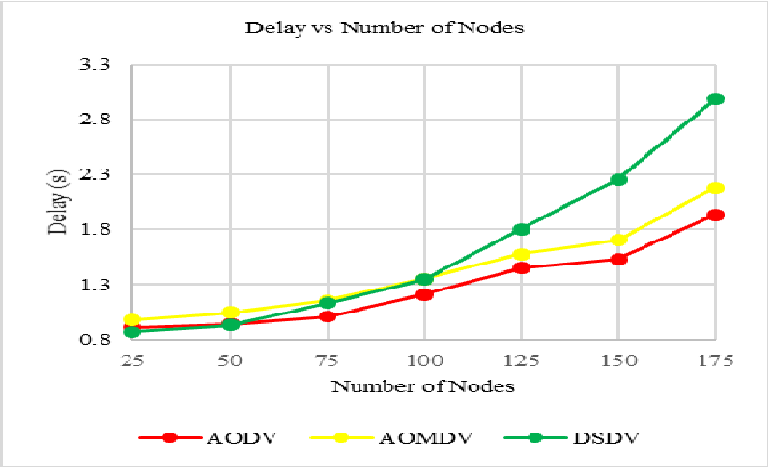


Figure 7. Average end-to-end delay.

Average End-to-End Delay (E2ED) is a measure of how fast a unit size of data can be transmitted across a network. E2ED is a sum of propagation delay, queueing delay, transmission delay, and processing delay at intermediate nodes. E2ED is influenced by node mobility and transmission distance. Frequent mobility and longer distances result in longer E2ED. In our simulations, the same mobility files were used in all three implementations to nullify the effects of mobility and distances when comparing E2ED performances. In all 3 implementations, E2ED increased as nodes increased; presented in *Figure 7* above. AODV and AOMDV showed similar trends as number of nodes increased. We attribute this to the On-demand nature of both routing protocols. AOMDV and AODV use similar route discovery mechanisms and deliver packets in a similar fashion; therefore, with the same mobility scenario they are expected to have similar E2ED. The extra delay recorded by AOMDV is because it spends additional time during each route discovery process to discover multiple routes. DSDV had the worst E2ED performance with a sharp rise in E2ED trend, as number of nodes increased. The observed difference is because, intermediate nodes spend longer processing delays as they check their route tables for next hops to forward data, whereas AOMDV and AODV use forward route setups resulting in less processing delays at intermediate nodes.

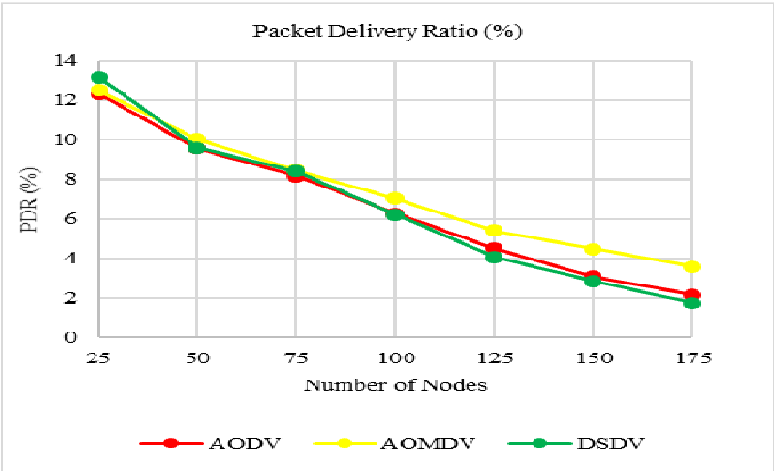


Figure 8. Packet delivery ratio.

Packet Delivery Ratio (PDR) is the ratio of delivered packets to the total number of packets generated. In *Figure 8* above, we expressed this ratio as a percentage. PDR is inversely correlated to Packet Loss Ratio. A higher packet delivery ratio means fewer packet loss. AOMDV proved to be the most reliable in terms of packet delivery. As mentioned earlier, AOMDV discovers multiple disjoint paths between source and destination. These disjoint paths are less probable to fail all at once; hence, a higher reliability in delivering packets from source to destination.

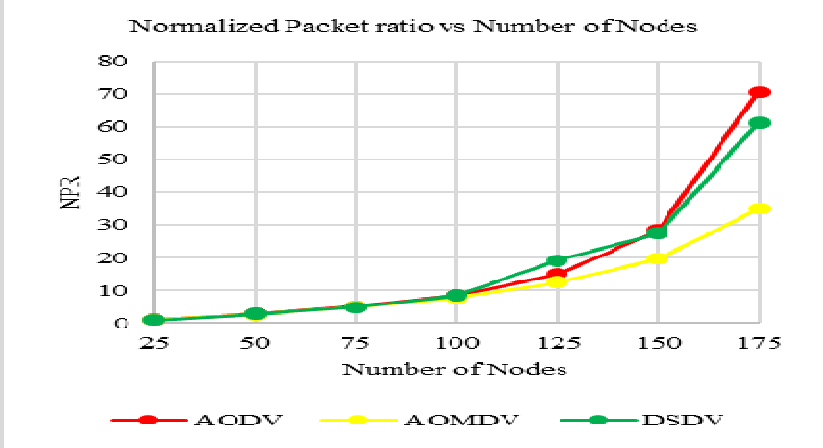


Figure 9. Normalized packet ratio.

Normalized Packet Ratio (NPR) is the ratio of control packets to actual data packets. NPR can be interpreted as the number of control messages needed by the MANET routing protocol, to send a single data packet from source to destination. A lesser NPR is most preferred in networks as control messages are not useful to end users. In *Figure 9*, it is observed that, all three protocols have similar trend and NPR values from 25 to 100 nodes. The significant difference in trend begins after 100 nodes. AOMDV had the best NPR performance whereas AODV recorded the worst performance. The observed pattern is attributed to the fact that, AODV nodes repeat the route discovery procedure each time a link is broken unlike AOMDV that resorts to a secondary path earlier discovered during the immediate past route discovery phase. It is only when all the multiple paths fail that AOMDV nodes repeat the route discovery procedure.

In *Figure 10* and *Figure 11* below, we zoom in on *Figure 9* to show a better picture of the trends between 25 and 100 nodes.

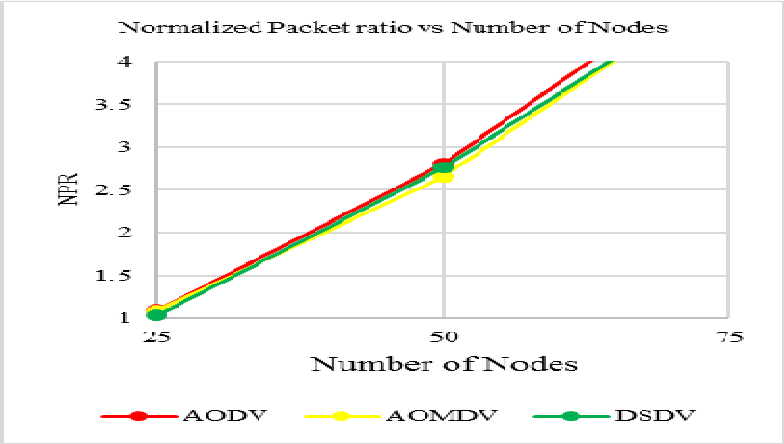


Figure 10. Normalized packet ratio (A).

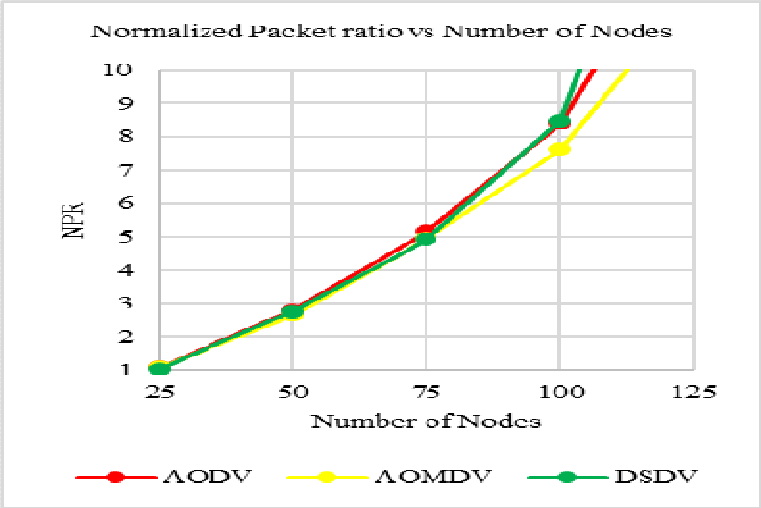


Figure 11. Normalized packet ratio (B).

5. CONCLUSIONS

We have presented a performance evaluation of Mobile IP on MANET. We have studied for the first time, the performance of Mobile IP on MANET using Ad Hoc On-demand Multiple Distance Vector (AOMDV) for routing packets inside the MANET. We have also studied the performance of Mobile IP using Destination-Sequenced Distance Vector (DSDV) and Ad Hoc On-demand Distance Vector (AODV) for routing packets inside the MANET.

We modelled Mobile IP on MANET using a wired cum wireless scenario in NS2. Our scenario included one Home Agent, a Corresponding Node and four Foreign Agents. Mobile nodes moved randomly between these sub networks and registered with an agent, whenever they entered a new sub network. Communication between Mobile Nodes and Corresponding Node continued even as Mobile Nodes moved across sub networks.

Results obtained from simulation suggested that, On-demand routing improved the performance of Mobile IP on MANET regarding; average end-to-end delay, throughput, packet delivery ratio, and normalized packet ratio. Specifically, Mobile IP on AOMDV outperformed AODV and DSDV.

ACKNOWLEDGEMENTS

We are grateful to God for the gift of life and good health throughout this study. We thank family, friends and colleagues for the support and encouragements thus far.

REFERENCES

[1] U. Jönsson, F. Alriksson, T. Lasson, P. Johansson, and G. Maguire, "MIPMANET - Mobile I P for Mobile Ad Hoc Networks," *MobiHoc '00 Proc. 1st ACM Int. Symp. Mob. ad hoc Netw. Comput.*, pp. 75–85, 2000.

[2] C. E. Perkins, "Mobile networking through mobile IP," *IEEE Internet Comput.*, vol. 2, no. 1, pp. 58–69, 1998.

[3] H. Lei and C. Perkins., "Ad Hoc Networking with Mobile IP," in *2nd European Personal Mobile Communications Conf. (EPMCC 97), IEE.*, 1997, p. 197–202.

[4] U. Jönsson, F. Alriksson, T. Larsson, P. Johansson, G. Maguire, and Jr, "MIPMANET: mobile IP for mobile ad hoc networks," *MobiHoc '00 Proc. 1st ACM Int. Symp. Mob. ad hoc Netw. Comput.*, pp. 75–85, 2000.

[5] E. M. Belding-Royer, Y. Sun, and C. E. Perkins, "Global Connectivity for IPv4 Mobile Ad hoc Networks, IETF Internet Draft." Work in progress, 2001.

[6] J. Xi and C. Bettstetter, "WIRELESS MULTIHOP INTERNET ACCESS : GATEWAY DISCOVERY , ROUTING , AND ADDRESSING," *Proc. Int. Conf. Third Gener. Beyond*, 2002.

[7] A. A. Hamidian, "A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS 2," no. January, 2003.

[8] R. Wakikawa, J. T. Malinen, C. E. Perkins, A. Nilsson, and A. J. Tuominen, "Global Connectivity for IPv6 Mobile Ad hoc Networks, IETF Internet Draft." Work in progress, 2001.

[9] E. Hassan, A. Alsaied, S. M. Alshareefmodatheir, and I. Hal, "Performance Evaluation of Mobile IP with DSD V Routing Protocol using NS2," 2015.

[10] S. N. Mane, N. V. Mane, and D. G. Khairnar, "Performance of mobile node between different MANET with Mobile IP," *2015 Int. Conf. Ind. Instrum. Control. ICIC 2015*, no. Icic, pp. 1662–1664, 2015.

[11] R. P. Salim and R. Rajesh, "A Survey: Optimal Node Routing Strategies in MANET 1 1," pp. 260–267, 2016.

[12] F. Maan and N. Mazhar, "MANET routing protocols vs mobility models: A performance evaluation," *2011 Third Int. Conf. Ubiquitous Futur. Networks*, pp. 179–184, 2011.

[13] D. G. Reina *et al.*, "A survey on ad hoc networks for disaster scenarios," in *Proceedings - 2014 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2014*, 2014, pp. 433–438.

[14] M. M. N. Aldeer, "A summary survey on recent applications of wireless sensor networks," *Res. Dev. (SCOReD), 2013 IEEE Student Conf.*, no. December, pp. 485–490, 2013.

[15] J. Jubin and J. D. Tornow, "The Darpa Packet Radio Network Protocols," *Proc. IEEE*, vol. 75, 1987.

[16] S. Toumpis and D. Toumpakaris, "Wireless ad hoc networks and related topologies: applications and research challenges," *e i Elektrotechnik und Informationstechnik*, vol. 123, no. 6, pp. 232–241, 2006.

[17] R. Ruppe, S. Griswald, P. Walsh, and R. Martin, "Near Term Digital Radio (NTDR) System." IEEE, pp. 1282–1287, 1997.

[18] M. P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic, "A survey of military applications of wireless sensor networks," *Mediterr. Conf. Embed. Comput. 2012*, pp. 196–199, 2012.

[19] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numer. Math.*, vol. 1, no. 1, pp. 269–271, 1959.

[20] T. J. Misa, "An interview with Edsger W. Dijkstra," *Commun. ACM*, vol. 53, no. 8, p. 41, 2010.

[21] R. Bellman, "On a routing problem," *Quart. Appl. Math.*, vol. 16, pp. 87–90, 1958.

[22] C. E. Perkins, "Ad Hoc Networking," p. 370, 2000.

[23] T. Stoilov and K. Stoilova, "Routing algorithms in computers networks," pp. 1–6, 2005.

[24] C. E. Perkins and P. Bhagwat, "Highly Dynamic (DSDV) for Mobile Computers Routing," *Proc. ACM SIGCOMM94, London, UK*, pp. 234–244, 1994.

[25] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," *Proc. - WMCSA'99 2nd IEEE Work. Mob. Comput. Syst. Appl.*, pp. 90–100, 1999.

[26] T. Larson and N. Hedman, "Routing Protocols in Wireless Ad-hoc Networks - A Simulation Study," *Event (London)*, 1998.

[27] M. K. Marina and S. R. Das, "Ad hoc On-demand Multipath Distance Vector Routing," *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, no. 3, pp. 92–93, 2002.

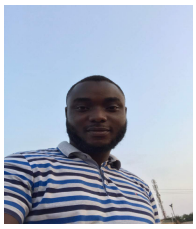
[28] A. Moravejosharieh, H. Modares, R. Salleh, and E. Mostajeran, "Performance Analysis of AODV , AOMDV , DSR , DSDV Routing Protocols in Vehicular Ad Hoc Network," *Res. J. Recent Sci.*, vol. 2, no. 7, pp. 66–73, 2013.

[29] S. Deering and Ed., "ICMP Router Discovery Messages," no. RFC 1256. pp. 1–19, 1991.

[30] C. E. Perkins, "IP Encapsulation within IP," no. RFC 2003. pp. 1–14, 1996.

[31] C. E. Perkins, "Minimal Encapsulation within IP," no. RFC 2004. pp. 1–6, 1996.

AUTHORS



Kingsley K. Ofosu is currently an MPhil student at the Department of Computer Science, University of Ghana. He received his BSc. degree in Psychology and Computer Science (Combined) from University of Ghana in 2013. His research interests include mobile networks, cloud computing and intelligent systems.

Jamal-Deen Abdulai received his BSc. degree in Computer Science in 2002 from the Kwame Nkrumah University of Science and Technology (KNUST). In 2006, he was awarded an MPhil and later in 2009 a PhD in Computer Science by the Department of Computing Science at the University of Glasgow, UK. Dr. Abdulai's is currently a lecturer at the Department of Computer Science, University of Ghana, investigating how probabilistic methods can be used to optimize the performance of both wired and wireless networks. His research interests include Performance modelling and evaluation of Mobile Wireless Ad hoc and Sensor Networks, Network Security and Management, Embedded Systems, Parallel and Distributed Systems, Artificial Intelligence and its application in information security.

Ferdinand A. Katsriku is the current head of the department of computer science, University of Ghana. In 1989, he received an M. Eng. in computer systems engineering with distinction from Kharkov Polytechnic Institute. He was awarded an MSc in Laser Engineering and Pulsed Power Technology in August 1992 and later awarded postgraduate certificate in education from King's College London in 1996. In 2000, he received a PhD in Information Engineering from City University, London. His current research interests are wireless sensor networks, cognitive radio and water quality monitoring. He is also a technical Reviewer of EPSRC grants and for major publishers including John Wiley and Elsevier.