Mobile Information Systems 6 (2010) 49–63
DOI 10.3233/MIS-2010-0092
IOS Press

Architecture for mobile Heterogeneous Multi Domain networks

Arjan Durresi[a], Ping Zhang[a], Mimoza Durresi[a,*] and Leonard Barolli[b]
[a]*Department of Computer and Information Science, Indiana University Purdue University Indianapolis, Indianapolis, IN 46202, USA*
[b]*Department of Information and Communication Engineering, Fukuoka Institute of Technology* (*FIT*), *3-30-1 Wajiro-Higashi, Higashi-ku, Fukuoka 811-0295, Japan*

Abstract. Multi domain networks can be used in several scenarios including military, enterprize networks, emergency networks and many other cases. In such networks, each domain might be under its own administration. Therefore, the cooperation among domains is conditioned by individual domain policies regarding sharing information, such as network topology, connectivity, mobility, security, various service availability and so on.

We propose a new architecture for Heterogeneous Multi Domain (HMD) networks, in which one the operations are subject to specific domain policies. We propose a hierarchical architecture, with an infrastructure of gateways at highest-control level that enables policy based interconnection, mobility and other services among domains. Gateways are responsible for translation among different communication protocols, including routing, signalling, and security. Besides the architecture, we discuss in more details the mobility and adaptive capacity of services in HMD. We discuss the HMD scalability and other advantages compared to existing architectural and mobility solutions. Furthermore, we analyze the dynamic availability at the control level of the hierarchy.

Keywords: Network architecture, mobility, policy based networking, heterogeneous networks

1. Introduction

Multi domain networks (MDN) can be applied in multiple scenarios, including military networks in battlefields, enterprize and campus networks, and so on. For example, the Internet is the biggest example of multi domain networks, where domains are the Autonomous Systems (AS).

One major characteristic of multi domain networks is that their domains are under different administrations. While such administrations might agree to share and collaborate on some services, for example the connectivity, they might not be willing to share all details of their networks, such as configuration, topology, name structures, routing details, mobility, security, and so on. For example, in today's Internet, routing is no longer based on algorithmic optimization but has to deal with policy compliance; the reason is that the Internet is build as network among AS, which are under different administrations. Whereas in the Internet AS are stable and their inter agreements regarding connectivity and traffic management are static, the domains and their relations in MDNs might be highly dynamic.

The best examples of MDN are military networks on battlefields, due to their highly dynamic changes, extreme requirements about policy control, and so on. However, other type of networks, such as enterprize and disaster response networks, are also the target of our proposed solutions.

[*] Corresponding author. Tel.: +1 317 274 8942; Fax: +1 317 274 9747; E-mail: durresi@cs.iupui.edu.

The militarys dependence on interacting networks in the physical, information, cognitive, and social domains is clear from its effort to transform itself into a force capable of network-centric operations [2, 3].

It is believed that global communications will fundamentally transform the conduct of war in the 21st century just as air power transformed it between World Wars I and II. This belief is embedded in two strategic assumptions of profound military significance. First, better situation awareness and communication in combat situations will result in higher combat effectiveness. This implies facile and high-bandwidth communications between elements of all services in combat operations as well as shared information in a common formant. Second, it is assumed that better situational awareness will make forces more mobile by allowing heavy armor to be replaced by agility. These assumptions underlie the transformation of military forces from the Industrial Age into the Information Age.

To win the battle of the future, the integration and networking of command, control, communications, computers, intelligence, surveillance, and reconnaissance systems is essential, from concept development to combat in the field. None of the systems stands alone on the battlefield. Another difficult issue is to adapt the highly centralized and hierarchical military command structure to the new generation of technologies. For example, it will be needed to network unmanned vehicles, include remote sensors and weaponry, while keeping responsible and accountable human beings in the loop.

Of particular interest are tactical level communications and networking challenges that require less operator intervention and provide greater and more seamless capabilities than exist in the current networks. Future battlefields require solutions to enable greater horizontal connectivity between tactical edge platforms and users in order to improve the timely transmission of command and control information across the battlespace. These tactical networks exhibit an essential dynamic nature and must support quick response entry and exit. The nodes on the network will have varying capabilities and might belong to network domains, which differ from routing, signalling, type of links, security level, administration, and so on.

Good candidate for MDN, which share most of the characteristics of military networks, are enterprize networks; such networks span over multiple locations, departments, or business functions. Various domains of such networks might need to control the interrelations with other domains based on specific policies, for example marketing domain might not be allowed to share specific information with research domain, or mobile nodes might have different privileges, depending in which domain they are located and so on.

Another example of MDN are networks build during disaster situations, requiring national or international relief interventions. For example, in a disaster area caused by a hurricane or a tsunami, many national of international entities might be involved; such entities might have their own type of networks, which on one hand might not be fully compatible with each other, and on other hand, various entities might not be willing to share all details of their networks. Therefore, a hierarchical controlled cooperation would be preferred.

We present a new Heterogeneous Multi Domain (HMD) network architecture and related protocol for seamless intercommunications among different network domains. HMD architecture enables policy based control over MDNs. We extend our presentation on mobility of nodes among domains and dynamic availability at control level.

The HMD architecture is shown in Fig. 1. The network is covered by various network domains, which are composed of wired or wireless links, of different technologies, and are managed by different entities. Interdomain communication is done by using a network of supernodes called *Gateways*. Gateways form the *control level* and are able to translate among different routing, signalling and security protocols

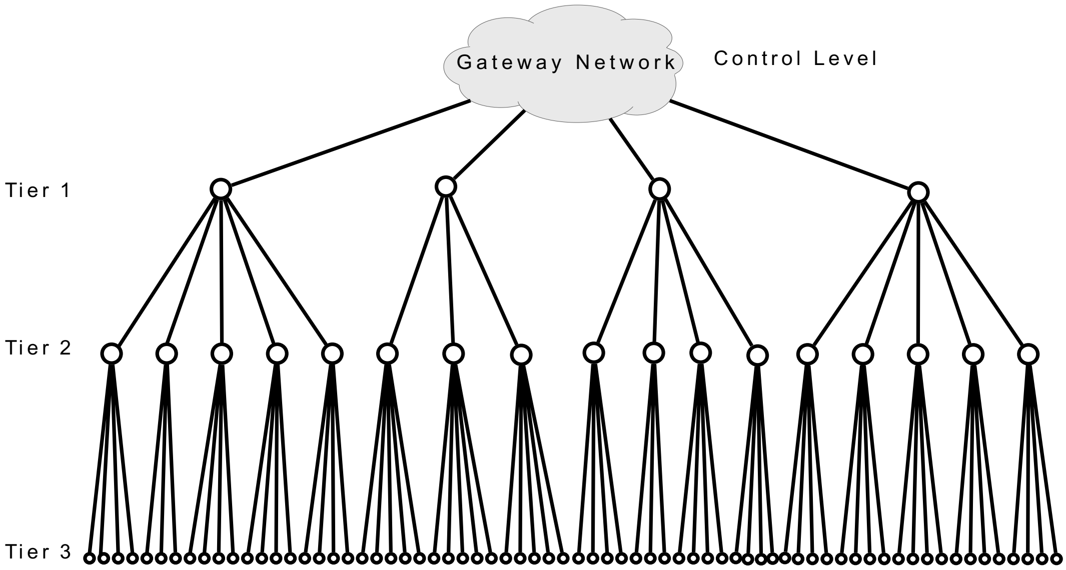


Fig. 1. Heterogeneous Multi Domain architecture.

used in various domains. The network among gateways has high connectivity, possibly a full mesh network. Therefore, routing among gateways is simple and support high QoS. Each domain can use one or more gateways for interdomain communications. The number of gateways per domain depend on the size of domains, their technology, and the level of demand for inderdomain communications. Also the number of gateways and their capabilities will adapt to changing needs in battlefield. Therefore, HMD architecture supports decentralized, dynamic, mission-driven, policy-based network management effective in the command operations center, as well as deployed and detached operations, and continuous network adaptation of mobile networks, and secure solutions.

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 presents HMD architecture. In Section 4 we present our solutions for mobility and security based on domain policies. In Section 5 we analyze the adaptation of capacity of gateways to the traffic need. Section 6 concludes the paper.

2. Background work

In [21] the authors developed a communications server provides realistic tactical mobility models.

In [36] the author surveys the components and characteristics of the Army's legacy communications networks, illustrates the directions currently being taken for accomplishing this digitization, describes the areas in which the civilian and military systems differ, and defines a glide path for convergence of the two technologies in support of the military's increasing need for information. Furthermore, the author argues that todays military communications networks cannot support the growing demand for information services on the battlefield. Video teleconferencing, electronic messaging and internetworked data services will require many changes in battlefield communications. These capabilities are critical for providing the decisive edge on the 21st century battlefield, for enhancing coordination, and for providing the future warfighter with an additional combat multiplier.

Traditional tactical communications systems consist of a number of separate subsystems with little interworking between them and with external sensors and weapons systems. Combat net radio (CNR) has provided the high-mobility communications required by combat troops, while trunk communications systems have provided high-capacity communications between headquarters at the expense of mobility.

In [35] the authors focus on new, information-age technologies that promise to offer seamless integration of real-time data sharing, creating a single logical network architecture to facilitate the movement of data throughout the battlespace. Because the structure of this network is constrained by the fundamental trade-off between range, mobility and capacity that applies to all communications systems, this network is unlikely to be based on a single network technology. In [35] it is presented an architecture for this network, and shown how its subsystems can be integrated to form a single logical network.

In [7] the author studies the dissemination of sensor data (reports) from the sensor network to the mobile ground forces (soldiers) for sensor gateways deployed in a battlefield scenario. Two schemes for propagating sensor reports are presented. In a centralized approach, all sensor reports must go through one designated node (command post). In a distributed approach, the network routes sensor reports directly to the soldiers. In a generic soldier mobility model, soldiers move in small groups (squads) along a line to random destinations on the battlefield.

The ad hoc wireless network is one of the most promising architectures for mobile networks. A mobile ad hoc network is a group of mobile, wireless nodes that cooperatively and spontaneously form a network. This network is independent of any fixed infrastructure or centralized administration.

Routing protocols in fixed networks have used algorithms that were traditionally based on link-state or distance-vector-type routing [16]. The common strategy in these algorithms is that each node forwards the message via the "shortest path". The concept of shortest path can be related to the number of hops, link utilization or queuing delay. A good survey about novel network architectures is presented in [29].

Due to the nature of ad hoc wireless networks, the above-mentioned routing protocols, which have a high complexity, cannot be used anymore. In wireless links the message complexity must be low, because of the limited bandwidth and the routes must be found quickly, as the topology is probably changing rapidly. The traditional link-state and distance vector routing protocols are not any more effective in this environment [12,34]. In [17] we discuss the performance of routing protocols for ad hoc wireless networks. In ad hoc wireless networks various division in cluster are used. In [5] we discuss the performance in selecting cluster heads. In [1] are discussed issues related to multi domain networks, and especially workload scheduling.

Network-wide broadcast is an essential feature for wireless networks. The simplest method for broadcast service is flooding. Its advantages are its simplicity and reachability. However, for a single broadcast, flooding generates abundant retransmissions resulting in battery power and bandwidth waste. Also, the retransmissions of close nodes are likely to happen at the same time. As a result, flooding quickly leads to message collisions and channel contention. This is known as the broadcast storm problem [28]. A good classification and comparison of most of the proposed protocols is presented in [40].

In [11] we have proposed a solution for authentication in heterogeneous networks. In [25] is discussed the problem of timely packet transmission in a wireless soft real-time system such as one would find on the battlefield.

Some of the proposed solutions that can be considered as competing with our solutions are discussed in the following.

The 4D architecture [14,15,41] and its extension, CONMan architecture [13], design a new management and control plan for the Internet. The 4D architecture mostly addresses the routing related management issues and those that apply to management and control within an autonomous system. However, each autonomous system (AS) of the Internet applies its own policies, including routing and access functions. In 4D architecture such policies have to be distributed to each element of the AS network. Therefore, applying inter AS or inter domain policies is not easy and any change in topology of policies requires all node updates, which will result in high overhead and scalability problems. Furthermore, the distribution of policies at lower nodes exposes policies to high security vulnerabilities. In our solution, the policies are applied at the higher level of the network hierarchy and single nodes, in most cases, are not aware of such policies. Therefore, applying the policies, in our solution is easier and safer than in 4D.

Maestro [27] proposes an operating system like approach for network control and management, where network controls are implemented as applications over an operating environment. The Maestro environment provides support to the network control applications much in the same way an operating system provides support to the applications, by providing services such as, scheduling, synchronization, interapplication communication, and resource multiplexing. But Maestro requires that, at least, the higher level of hierarchy of the multi domain network apply the same "operating system," which is not realistic in our scenarios of multi domain networks.

Autonomic Network Architecture (ANA) project [37] proposes self-configuring nodes that self-organize into a network system through neighbor interactions, with multiple such systems self-federating into a heterogeneous Internetwork. In-Network Management (INM) [10,33] proposes an architectural design for embedding management capabilities in all network entities and the management functionalities that can be achieved as a result of their collaboration. Again, such architectures are not realistic for multi domain networks, where domains are independent of each other and their cooperation is based on their individual policies.

Mobility has been one of the major concerns in the design of network architectures. Therefore, extended efforts have been dedicated to design efficient and practical solutions for mobility. Mobile IP (MIP) [19,31,**?**] and its enhancements [4,30] are among the most popular solutions to support mobility. MIP-like solutions need modifications on access networks and support from service providers [8,20]. MIP suffers also from non optimal routing and triangulation.

The Host Identity Protocol (HIP) [23,26] is an architecture that separates identifier and IP address by introducing Host Identity (HI). HI is initially acquired by DNS lookup, and mobile node keeps updating peers and DNS record during move. HIP provides integrated end-to-end host mobility and security, but mobility management is left open. For highly mobile nodes a type of rendezvous server is proposed, though the role of rendezvous deployment could be questioned.

FARA [9] is an abstract high level architecture model aimed to provide general guidelines and a flexible framework for clean slate Internet architecture. Mobility is one of the major concerns of FARA, and it is primarily addressed by ID/locater split. FARA suggests to use rendezvous point to setup initial connection to mobile node, or use directory service (fDS) to lookup and keep track of mobile node, though the mechanism is left empty. However, MIP, HIP and FARA solutions do not support domain mobility controlled by policies at domain level.

In this paper we propose a new Heterogeneous Multi Domain (HMD) architecture and related protocols. In HMD architecture all operations, including mobility, connectivity, security and so on, are dynamically controlled by policies specified at the highes level of network hierarchy, called control level.

Our solution provides QoS in communications, making possible the diversity of services for different nodes, service prioritization and real-time communication among various domains.

3. Heterogeneous Multi Domain (HMD) architecture

Various types of network domains operate in modern battlefields, as shown in Fig. 1. For example, various elements of military forces, such as army, navy, air forces, and special units cooperate to achieve specific tactical goals. Each one of these organizations has its own network structure in one or more domains. The intercommunication among domains under different administrations is not at all trivial. Different domains might use different routing, signalling and communication protocols. Domains could be wired or mostly wireless based. They might be using different wireless architectures such as IEEE 802.11, WaMAX, infrastructure based or ad hoc ones, and so on. Domains might differ in size, offered services, security policies and protocols. Furthermore, such characteristics can unpredictably change during the battle events. For example, in particular moments the needs for interdomain communications in a given domain can be increased significatively. In other occasions, the required level of QoS could be necessary. Therefore, the interdomain network should be ready to adapt and satisfy such requests.

Another realistic scenario is that of cooperation among allied arm forces in the same battlefield. In this case, besides the above mentioned challenges, intercommunications should be strongly policy-based. While allies need to communicate, they would like to keep strict control about resource and intelligence sharing.

In HMD architecture, interdomain communications are realized by a network of gateway nodes, called control level. Gateways are special supernodes that communicate with their own domains and among themselves. A domain could have one or more gateways, and this number can change dynamically depending on needs for interdomain communications.

In the following we describe in greater detail the elements of HMD architecture and their major responsibilities.

3.1. Nodes and domains

In HMD architecture no constrains are posed regarding the type of nodes and their network domains. In most of the cases such domains will be wireless networks of different types, such as infrastructure based or ad hoc ones, for examples IEEE 802.11 family, ad hoc networks, sensor networks and combinations of them.

The nodes could be stationary or mobile, such as portable or wearable devices by soldiers, vehicles, maned and unmanned aircrafts, floating and underwater devices, and so on. In the following we describe the node's responsibilities:

- Depending on the case, nodes in the same domain exchange information to fulfill their tactical operation goals. For example, sensors collect information and send it to their sinks, soldiers communicate with their commanders, etc. However, inderdomain communication is necessary at tactical level. For example, soldiers or vehicles need to collect directly information from sensor sinks; terrestrial forces will need tight local coordination with air force to avoid friendly fire. The same is true among allied forces.
- Nodes have a personal Identity (ID). Node's ID is unique in the whole network. ID could have several parts that reflect various organizational hierarchies. Besides ID, a node in a given domain has a node domain address with several fields, such as *Domain ID*, *node address*, and *other parameters*.
- Intra domain routing will be done using node domain addresses.
- Inter domain routing will be using node domain address or node's ID. The use of node ID is especially useful in case of moving nodes among various domains. When a node moves to a given domain,

the node contacts the domain gateway and receives a node domain address. At the same time the gateway updates the gateway network database with the mapping of the node ID and its node domain address.

- To communicate with other nodes in other domains, a given node first locates and than communicates with the appropriate gateway.

3.2. Gateways

In general, gateways have more recourses than other nodes. On one hand, gateways are able to communicate will part or all g nodes of a given domain, or several domains. Gateways are installed topically in aircrafts, ships, satellites, tanks and so on. On the other hand, gateways form a highly connected high bandwidth network among themselves. In the following we describe in more detail gateways and their network responsibilities:

- Gateways will advertise themselves to nodes of a given domain. Most importantly, gateways will authenticate themselves to the nodes. The details of such protocols are outside of the scope of this paper.
- Gateways are able to run different communication protocols, in order to interact with several domains. There are two reasons for this: *First*, in continues changing conditions and topologies, a gateway could be close to various domains; and *Second*, in order to satisfy mission oriented QoS, adaptive load balancing among gateways might be needed, therefore they should be able to communicate with several domains.
- Gateways will handle inderdomain mobility. A given node could move from one domain to another. The appropriate gateway will provide necessary authentication and security information to the mobile node in order to be accepted in the domain. Furthermore, gateways will keep track of the correct mobile nodes' locations among domains. Therefore, gateways will locate and map the node ID to its current node domain address. For example, nodeA, in a given domain, needs to communicate with nodeB. However, nodeA doe not know in which domain is currently nodeB. Therefore, nodeA contacts its gateway and ask to communicate with nodeB. The gateway network knows in which domain is nodeB, and forward the request there.
- Gateways translate between the protocols used by interdomain nodes that are communicating. Therefore, nodes send their packets following the protocol of their own domain, and gateways will do the needed translation. the translation from one protocol to another is not always trivial. The details of such translation are out of the scope of this paper.
- A very important role for gateways and their network is administrative and policy management. While it it desirable seamless communication among nodes of different domains, it is very important that such communications and their security aspect follow policies and rules decided by domain administrators. For example, not all services of a given domain might be available to other domains; allied domains might want to restrict interconnections and exchange of data. Gateways will support in applying security policies in per domain and per connection basses.
- Gateway networks will adapt to traffic requirements, based on missions and tactical situation in battlefield. For example, the number of gateways will change depending on the needs of domains for interdomain bandwidth and the QoS. Furthermore, gateways will provide differentiated service to different types of traffic. The final goal is to optimally satisfy users need by using all available network resources.

3.3. Inter domain routing

HMD architecture supports two types of interdomain routing:

Point-to-Point Communications. This algorithm defines the action of nodes and gateways communications between a source and a destination that are in different domains.

Broadcast Communications. This algorithm defines the action for partial or full broadcast communication in one or more domains. The hierarchical structure of HDM is in particular suitable for broadcast communications. In this case, one or more gateways can broadcast the message over the destination domain.

Routing for Point-to-Point interdomain communications can be done based on the destination node address or node ID. The latter case is more suitable for highly mobile nodes. We first discuss routing based on network address.

The *node address* will be structures to include: *Domain ID* and *node address* in that domain. So when node *x* of domain *A* need to send a packet to node *y* of domain *B*, it will forward the packet to one of the available gateways. The gateway, first will consult the policy database regarding communications among domain *A* and *B*, and nodes *x* and *y* of such domains. In case the communication is allowed, the gateway will do the needed protocol translation and adaption, and will forward the packet to the appropriate gateway that covers domain *B*. The latest gateway will forward the packet to node *y*.

When routing is done based on destination node ID, the corresponding gateway after receiving the packet has to locate the destination node, by consulting the location database updated by all gateways. In this database to each node ID corresponds the current node address. Later the communication continues based on the founded node address.

We stress that HMD is very scalable. Independently of the number of nodes and domains the number of needed messages is the same for each communication. In case of routing based on network address there are three messages involved and one protocol translation. When routing is based on node ID, one more location database reading is needed.

4. Policy based mobility and security

In MDN nodes could move from one domain to another. In such cases the moving nodes and other nodes might need to communicate. We present in the following our solution for policy based mobility and security that enables a tradeoff range between overhead and security.

We assume that each node in the network has a profile at his original server inside its domain. A profile consists of two parts: the invariant part which includes user ID, authentication information, contract information, etc; the other comprises variant information such as location information and current status, plus the administration information of the domain where the node is currently in. The original server issues the profile, and manages all information contained in the invariant of profile. This part profile is signed by the original server that protect it from being modified by others. The original server also has capability to invalidate the previous or expired profile. The variant part is updated by the the domain hosting the mobile node, and the administration information is included as well.

When the node moves to another domain, the node updates its profile with the new location (address assigned in the present location). Furthermore, the node's profile replica could propagate or not, depending on the applied policy) to other domain servers at various levels of hierarchy. The profile replicas are distributed based on the history of the node's moves (updates) and requests for communication from other nodes (lookups). The copy of original profile is always stored at the original server.

In HMD architecture, in order to communicate with a mobile node, peer nodes will need to access the mobile node's profile to locate it and retrieve authentication information. The mobile node will keep updating its profile when it moves to a new place and a new network address is assigned. Servers, which are deployed at each level which hold a replica of the mobile node's profile, may make decision whether grant or reject the lookup request from local nodes. The replication algorithm runs on these servers to dynamically adjust the replication status of the mobile node's profile.

In HMD architecture, the whole mobility management system follows the hierarchy-tree structure. Hence, firstly every cross domain request and response must go through the *Control Level* formed by the network of gateways. Therefore, the *Control Level* can impose the desired policies regarding cross domain replications of profiles. Furthermore, each gateway can check all replica communication of its descendant domains and make decision whether allow replica out to parent domain. For example, a node X belongs to a sub-domain B11. In order to secure X's location information to only recognized hosts in network, B11's gateway sets X's replication rules as X's profile cannot be propagated outside Domain B. Therefore no matter when X moves, any node in network that wants to resolute X's address must talk to a server in Domain B which holds X's profile replica, and servers within Domain B would follow the white and black list to determine whether serve the incoming request. The gateway of Domain B can filter out all possible leaks of X's profile.

Each gateway may have different replication rules of a specific profile or a group of profiles belong to its domain. In the case of necessity, the gateway can override the static rules defined in the profile, and this type of intervention is usually taken to prevent leak of profile or information. The revocation of existing replicas can also automatically spread along the replica tree, where the request propagates similar to a update request.

4.1. Replication algorithm

The network cost is used as one criterion for profile replication algorithm. The network distance is represented by hops $c(X,Y)$ between two locations X and Y, and the network cost is the sum of signaling distance. rendezvous server from an external directory (especially the case millions of rendezvous servers out there), and MIP may have triangle routing for all traffic. We define the number of update requests of mobile node A sent from location X as $u(A,X)$ and lookup request for A is $l(A,X)$. If the rendezvous or nearest server is in location Y, then the cost to send the update request is: $u(A,X) \cdot (c(X,Y))$. For HMD the total update cost including the cost to propagate to replica is: $u(A,X) \cdot (c(X,Y) + \sum_{r \in Replica} c(Y,r)$ when using unicast. For a given period, the total cost is: $\sum_{X \in Aenters} u(A,X) \cdot (c(X,Y))$ for HIP rendezvous mode, $\sum_{X \in Aenters} u(A,X) \cdot (c(X,Y) + \sum_{r \in Replica} c(Y,r)$ for HMD. The lookup cost for both HIP rendezvous and HMD is: $2 \times \sum_{X \in Request} l(A,X) \cdot c(X,Y)$, and Y is rendezvous server for HIP or nearest server for HMD.

We use the modified replication algorithm from [39]. The whole network is modeled as a tree. Each node of the tree represents a HDM server. Network cost, i.e. sum of hops, is computed as weight of requests. The online algorithm uses Lund's algorithm [24] with Smart Propagation. A offset vector is used to represent past information, by which replica state of a subscriber is determined according to defined state transition table. For one edge of a network level:

```
1: From request (either update or lookup) submitted locally or propagated from the other end of edges,
   adjust the offset vector $F$.
2: Set new replica state $S$ base on new offset vector $F$.
3: **if** receives lookup request **then**
```

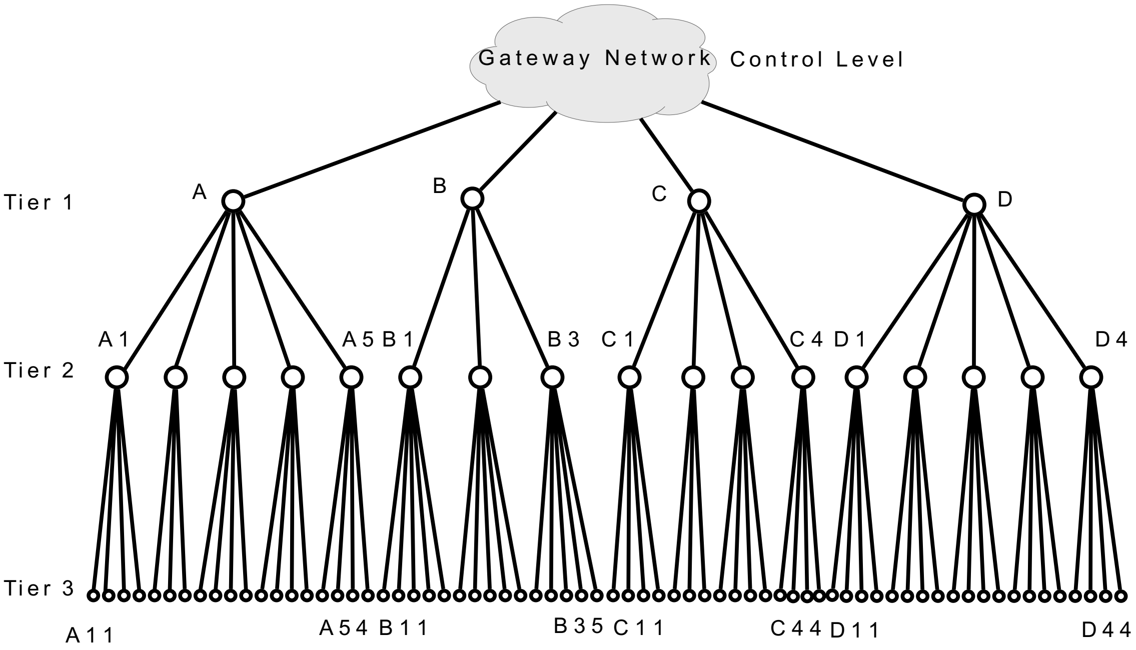


Fig. 2. Simulation topology.

```
    Propagate request to the other end if $F$ changes with a local replica.
else
    Propagate request to the other end if $F$ changes without a replica on the other end.
end if
```

4.2. Simulation of policy enforcement on mobility

The presented simulations are based on the policy enforcement discussed above, and the result in Fig. 3 clearly shows the trade off between level of security and network overhead or performance. We use an abstract topology model that has only network gateways as topology node and each gateway represents nodes and sub networks belong to it. The topology comprises of ten tier-1 gateways, 21 tier-2 gateways and 77 tier-3 gateways, as shown in Fig. 2. For simplicity only hierarchy connections are considered. Mobile node movement is represented as moving from leaf networks to leaf networks. Other nodes who want to talk to mobile nodes also reside in leaf networks.

HIP Rendezvous Server (RVS/HLR) model [22] is used as reference: each time a mobile node moves it will notify its rendezvous sever for a address update. Any peers of this mobile node that want to contact it need to initially talk to rendezvous server in order to be redirected to the mobile node, which actually is address lookup. In HMD various level servers will be used as replication servers under the control of gateways. As a result the replication tree of each mobile node's profile will dynamically be adjusted on the corresponding level servers.

For the simulation period, we assume that each mobile node will move 20 times. Each node will use a random walk move pattern, and moving distance is randomly generated complying to Binomial distribution with $p = 0.5, \lambda = 20$. (Here λ means tested for 20 times. Each time stands for a step and one step equals one leaf network. λ has no relation with the move times). During simulation one mobile

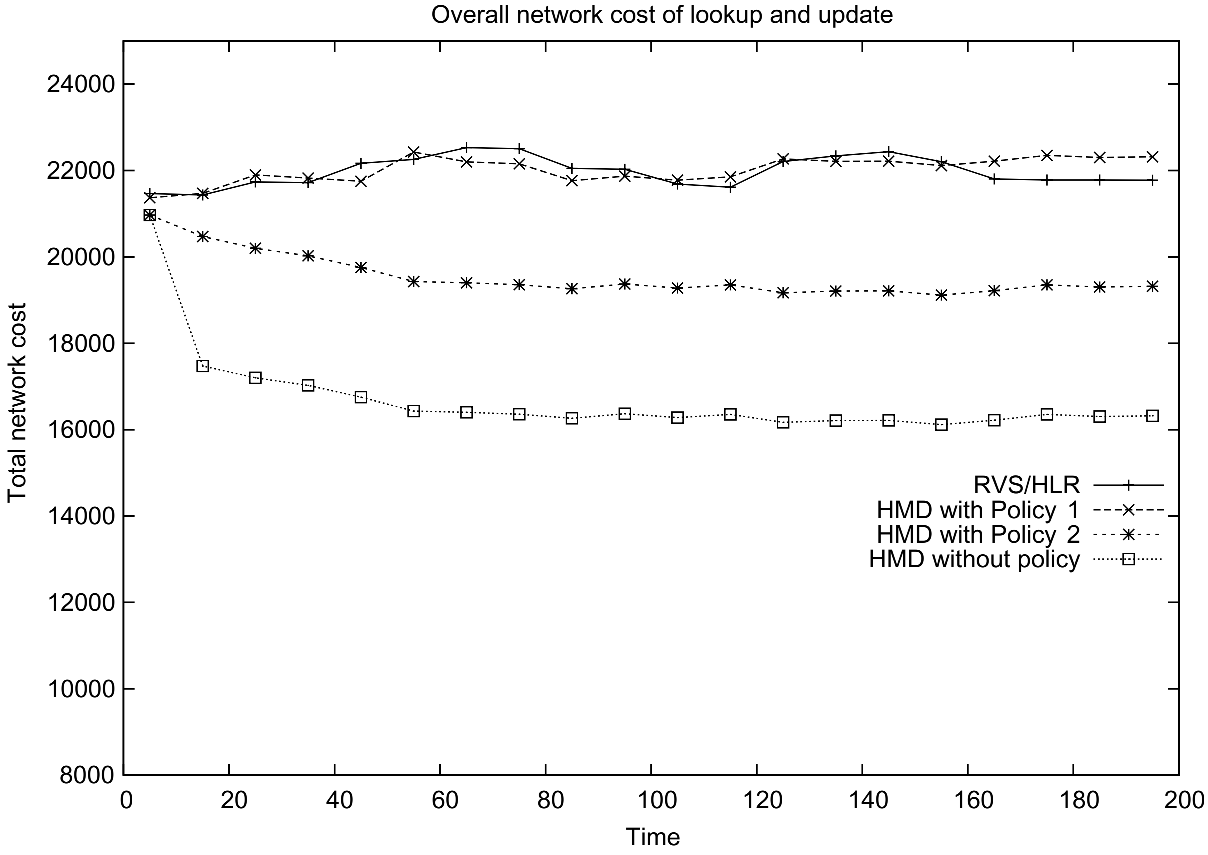


Fig. 3. Simulation results of policy enforcement.

node will be looked up for 200 times (which can be viewed as 200 peers and one time per peer, or 100 peers and two times per peer, etc.), for a 1:20 update/lookup ratio. The unit of time corresponds to events of lookup request, i.e. 20 units of time contains 20 lookups and one update request. The simulation process is repeated for 100 times, which represents 100 distinct mobile nodes, to gather enough amount of data in order to compensate the effect of skewed random number generation.

We run simulation on different level of security rules to test the tradeoff between performance and security, as shown in Fig. 3. From the result we can see that when there is no policy enforced that the replication can be freely adjusted among all servers, the HMD has less overall network cost compared to RVS/HLR solutions. In addition after initial replication tree adjustment HMD usually have much less lookup latency due to localized replica.

Then we enforce a harsh policy “1” which forbidden replication extending beyond A1. This policy de facto makes HDM similar to RVS/HLR except the possibility to set up replica in sub network of A1, if they could have enough lookup requests. The result is no surprise that HMD with policy “1” has similar network cost to RVS/HLR, and at some time even higher due to synchronization cost. However, this is the scenario of tight security enforcement such the if anyone wants to talk to a mobile node must acquire permission from it local server A1.

Next we enforce a policy “2”, such that the replication of mobile node’s profile is now allowed to extent over the *Control Level*. Since we assume the mobile node belongs to server A1 and its original profile is stored there, then under policy "2" the replica tree will stop extending at headquarter, which is enforced by headquarter server. Nodes and servers under network B, C, and D will have to query the gateways at *Control Level* to fetch profile of the mobile node, but nodes and serves in network A can still benefit from localized replica. For example, network A54 has a large amount of lookup requests and as a result a replica is set up at A5's server that reduces lookup request for all nodes and in network A5 and A5's sub network. The overall network cost is increased compared to HMD without policy, but still lower than RVS/HLR.

5. Dynamic capacity at control level

In this Section we will analyze and discuss the adaptation of gateway resources to the needs of interdomain traffic. Our goal is to show how the network can self adapt, by changing the number of gateways, to keep the QoS at the desired level.

When the traffic rate and its QoS requirements cannot be satisfied by a single gateway, other gateways can start to serve the domain. As a result the queuing probabilities and the waiting time for messages accumulated in every involved gateway will de decreased. By using the probability theory we can calculate the improvement in the case of having a total of *m* gateways. Therefore, the system can adjust to the right number of gateways.

Let us suppose that for every involved gateway that the resultant of all incoming streams is an overall stream with arrival rate λc. Same way we will suppose that the messages are transmitted from one of the gateways with a Poisson transmitting rate: μ. In this case we have the case of *M/M/m* model [6] and we can calculate the queuing probability.

We model the system of *m* gateways in a domain by the *M/M/m* system [6]. The probability that a message arrival will find all gateways busy and will be forced to wait in queue is given by:

$$P_W = \Sigma_{n=m}^{\infty} p_n = \Sigma_{n=m}^{\infty} \frac{p_0 m^m \rho^n}{m!} = \frac{p_0 (m\rho)^m}{m!} \Sigma_{n=m}^{\infty} \rho^{n-m} \tag{1}$$

and finally by:

$$P_W = \frac{p_0 m^m \rho^n}{m!(1-\rho)} \tag{2}$$

where p_0 is give by Eq. (3). Equation (2) is known as the *Erlang C formula*.

$$p_0 = \left[\Sigma_{n=0}^{m-1} \frac{(m\rho)^n}{n!} + \frac{(m\rho)^n}{m!(1-\rho)} \right]^{-1} \tag{3}$$

The expected number of messages waiting in queue is given by:

$$N_W = \Sigma_{n=0}^{\infty} n p_{m+n} \tag{4}$$

In [6] it is shown that:

$$N_W = \Sigma_{n=0}^{\infty} n p_0 \frac{m^m \rho^{m+n}}{m!} = \frac{p_0 (m\rho)^m}{m!} \Sigma_{n=0}^{\infty} n \rho^n \tag{5}$$

Finally it can be obtained:

$$N_W = P_W \frac{\rho}{1-\rho} \tag{6}$$

The average waiting time W_m a message has to wait in queue when there are m gateways is:

$$W_m = \frac{N_W}{\lambda} = \frac{\rho P_W}{\lambda(1-\rho)} \tag{7}$$

The average delay per message is, therefore:

$$T_m = \frac{1}{\mu} + W = \frac{1}{\mu} + \frac{\rho P_W}{\lambda(1-\rho)} \tag{8}$$

Using $\rho = \frac{\lambda}{m\mu}$, we have:

$$T_m = \frac{1}{\mu} + W = \frac{1}{\mu} + \frac{P_W}{m\mu - \lambda} \tag{9}$$

while when there is only one gateway per domain the average delay would be:

$$T = \frac{1}{\mu - \lambda} \tag{10}$$

In the case of one gateway, when λ is slightly less then μ, the queue and consequently the delay is increased, as shown from Eq. (10). For the same λ, in the case of multiple gateways, we will have $\lambda < m\mu$. Therefore, in Eq. (9) P_W is small and the delay is close to $1/\mu$. On the other hand, if the load is higher, that means in the case of multiple gateways ($\lambda \approx m\mu$) the delay is given by Eq. (9), while if it was a single gateway the delay in this case becomes unbounded. Furthermore, Eq. (9) can be used to quantify the reduction in delay per hop in case there are *m* gateways in each domain.

In the case of multiple gateways, the q-Percentile of the waiting time is given by the following equation [18]:

$$max\left(0, \frac{W_m}{P_W} ln \frac{100 P_W}{100 - q}\right) \tag{11}$$

Using Eq. (11), we can optimize the efficiency of this protocol by adjusting the number of gateways used. So if we would like to satisfy the condition that 80 or 90 % of messages need to wait less than a desired amount of time we can find from Eq. (11) the desired number of gateways that we need to use.

We illustrate the tradeoff between traffic load, delay and number of gateways with the following example adapted from [38].

Suppose there is only one gateway serving a given domain. For the given arrival rate, the gateway is 40% utilized and giving acceptable performance (delay). Now, let us assume that the traffic rate is increased, how many gateways would be needed to keep the same performance. Let assume that the service time is 1 for convenience. Therefore, following *M/M/1* model, the original one single gateway must have an arrival rate $\lambda = 0.4$ to give $\rho = 40\%$ utilization, and the average waiting time in queue will be $W = 1.67$. Figure 4 shows how much multiple gateways can be loaded compared to single gateway. For example, if single gateway of 40% utilization is acceptable, we can load three gateway system up to 73% and obtain the same queuing delay. The ten system gateway can be loaded up to 90% for the same performance.

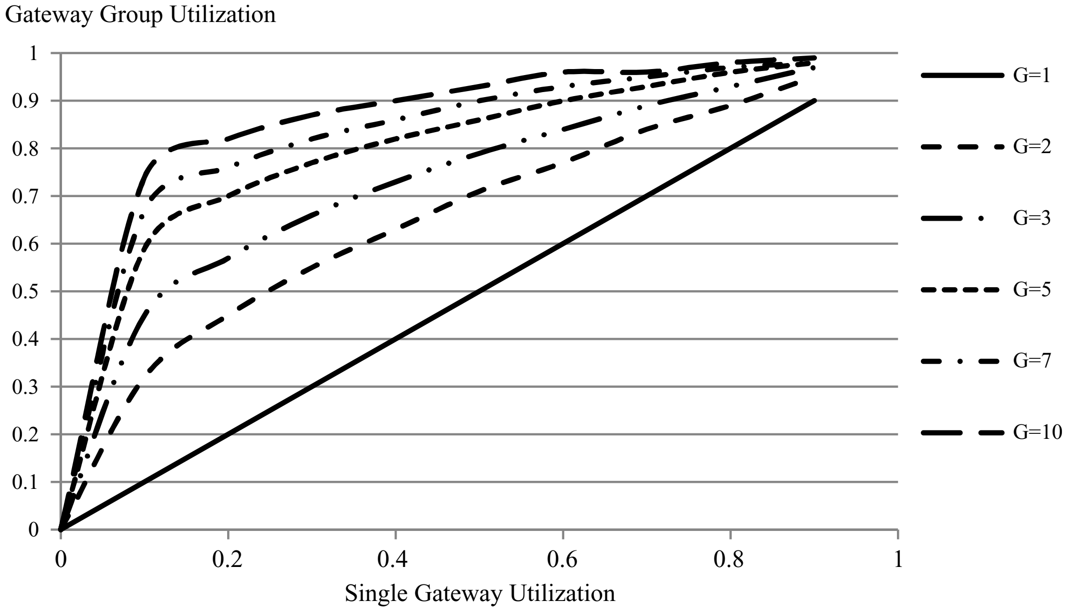


Fig. 4. Tradeoff among delay, traffic load and number of gateways.

6. Conclusions

We presented a new architecture for Heterogeneous Multi Domain (HMD) networks, which are under different administrations. HMD architecture enables operation controls based on domain policies. Therefore, routing, mobility, and security can be flexibly designed based on individual domain policy. We showed how our solution enables tradeoffs among network overhead and desired security level, following specific policies. Furthermore, HMD can dynamically self-adapt to traffic needs for bandwidth and QoS.

References

[1] IBM Tivoli Workload Scheduler Planning and Installation Guide. http://publib.boulder.ibm.com/tividd/td/TWS/SC32-1273-02/en_US/HTML/igmst42

[2] *Network Science*, Committee on Network Science for Future Army Applications, National Research Council, 2006.

[3] *ONR BAA-08-20 Dynamic Tactical Communications Networks*, Office of Navy Rresearch ONR, 2008.

[4] I.F. Akyildiz, X. Jiang and S. Mohanty, A survey of mobility management in next-generation all-ip-based wireless systems, In *Wireless Communications, IEEE*, volume 11, pages 16–28, August 2004.

[5] J. Anno, L. Barolli, A. Durresi, F. Xhafa and A. Koyama, Performance evaluation of two fuzzy-based cluster head selection systems for wireless sensor networks, *Mobile Information Systems* **4**(4) (2008), 297–312.

[6] D. Bertsekas and R. Gallager, *Data Networks*, Prentice Hall, Upper Saddle River, New Jersey, 1992.

[7] L. Briesemeister, Sensor data dissemination through ad hoc battlefield communications. In *Communication Networks and Distributed Systems Modeling and Simulation Conference* (*CNDS*), January 2003.

[8] M. Buddhikot, A. Hari, K. Singh and S. Miller, Mobilenat: a new technique for mobility across heterogeneous address spaces, *Mob Netw Appl* **10**(3) (2005), 289–302.

[9] D. Clark, R. Braden, A. Falk and V. Pingali, Fara: reorganizing the addressing architecture, In *FDNA '03: Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture*, pages 313–321, New York, NY, USA, 2003. ACM.

[10] D. Dudkowski, M. Brunner, G.Nunzi et al., Architectural Principles and Elements of In-Network Management, In *Proceedings of the Mini-conference at IFIP/IEEE Integrated Management symposium*, New York, USA, 2009.

[11] A. Durresi, M. Durresi and L. Barolli, Secure authentication in heterogeneous wireless networks, *Mobile Information Systems* **2**(4) (2008), 119–130.

[12] L.M. Feeney, A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks, In *Technical Report, Swedish Institute of Computer Science, ISRN:SICS-T-99/07-SE*, 1999.

[13] P. Francis and J. Lepreau, Towards Complexity- Oblivious Network Management, Technical Report NeTS-FIND Initiative, NSF.

[14] A. Greenberg, G. Hjalmtysson, D.A. Maltz et al., A Clean Slate 4D Approach to Network Control and Management, *ACM SIGCOMM Computer Communication Review* **35**(5) (October 2005).

[15] A. Greenberg, G. Hjalmtysson, D.A. Maltz et al., Refactoring Network Control and Management: A Case for the 4D Architecture, Technical Report Technical Report CMU-CS-05-117, CMU CS, September 2005.

[16] C. Huitema, *Routing in the Internet*, (2nd Edition), Prentice Hall PTR, New York, 2000.

[17] M. Ikeda, L. Barolli, G. De Marco, T. Yang, A. Durresi and F. Xhafa, Tools for performance assessment of OLSR protocol, *Mobile Information Systems* **2**(5) (2009), 165–176.

[18] R Jain, *The Art of Computer Systems Performance Analysis*, John Wiley & Sons, New York, 1991.

[19] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6, RFC 3775 (Proposed Standard), June 2004.

[20] J. Kempf, Goals for Network-Based Localized Mobility Management (NETLMM), RFC 4831 (Informational), April 2007.

[21] S.R. Kolek, S.J. Rak and P.J. Christensen, Battlefield communication network modeling. http://dss.ll.mit.edu/dss.web/98F-SIW-143.pdf.

[22] J. Laganier and L. Eggert, Host Identity Protocol (HIP) Rendezvous Extension, RFC 5204 (Experimental), April 2008.

[23] J. Laganier, T. Koponen and L. Eggert, Host Identity Protocol (HIP) Registration Extension, RFC 5203 (Experimental), April 2008.

[24] C. Lund, N. Reingold J. Westbrook and D. Yan, Competitive on-line algorithms for distributed data management, *SIAM Journal on Computing* **38**(3) (March 1999), 1086–1111.

[25] M.J. Markowski and A.S. Sethi, Wireless MAC protocols for real-time battlefield communications, In *IEEE MILCOM'97*, 1997.

[26] R. Moskowitz, P. Nikander, P. Jokela and T. Henderson, Host Identity Protocol, RFC 5201 (Experimental), April 2008.

[27] T.S. Eugene Ng and A.L. Cox, Maestro: An Architecture for Network Control Management, Technical Report NeTS-FIND Initiative, NSF.

[28] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen and J.-P. Sheu, The Broadcast Storm Problem in a Mobile Ad Hoc Network, In *Proceedings of ACM MOBICOM*, pages 151–162, Seattle, Washington, US, August 1999.

[29] S. Paul, J. Pan and R. Jain, Architectures for the Future Networks and the Next Generation Internet: A Survey, Technical Report 2009-69, Department of Computer Science and Engineering, Washington University in Saint Louis, October 2009.

[30] E. Perera, V. Sivaraman and A. Seneviratne, Survey on network mobility support. *SIGMOBILE Mob Comput Commun Rev* **8**(2) (2004), 7–19.

[31] C. Perkins, IP Mobility Support for IPv4, RFC 3344 (Proposed Standard), August 2002. Updated by RFC 4721.

[32] C. Perkins, P. Calhoun and J. Bharatia, Mobile IPv4 Challenge/Response Extensions (Revised), RFC 4721 (Proposed Standard), January 2007.

[33] A.G. Prieto, D. Dudkowski, C. Meirosu et al., Decentralized In-Network Management for the Future Internet, In *Proceedings of IEEE ICC?9 International Workshop on the Network of the Future*, Dresden, Germany, 2009.

[34] E. Royer and C.-K. Toh, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks, *IEEE Personal Communications Magazine*, pages 46–55, April 1999.

[35] M.J. Ryan and M.R. Frater, *Tactical Communications for the Digitized Battlefield*, Artech House Publishers, 2007.

[36] P. Sass, Communications networks for the force XXI digitized battlefield, *Mobile Networks and Applications* **4**(3) (October 1999), 139–155.

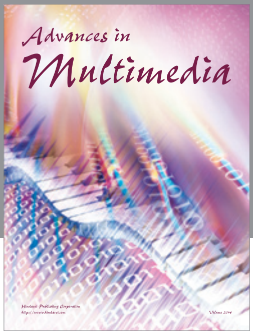
[37] M. Shell, Autonomic Network Architecture (ANA) Project, 2009.

[38] M. Tanner, *Practical Queueing Analysis*, McGraw-Hill, Cambridge, UK, 1995.

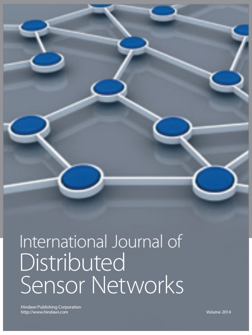
[39] K.Q. Tian and D.C. Cox, *Mobility Management In Wireless Network: Data Replication Strategies and Applications*, Kluwer Academic Publishers, Boston, December 2004.

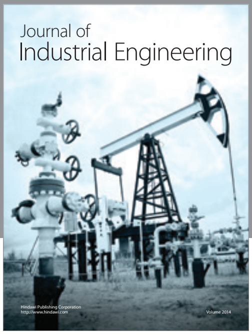
[40] B. Williams and T. Camp, Comparison of broadcasting techniques for mobile ad hoc networks. In *Proceedings of the third ACM international symposium on Mobile ad hoc networking & computing*, pages 194–205, Lausanne, Switzerland, June 2002.

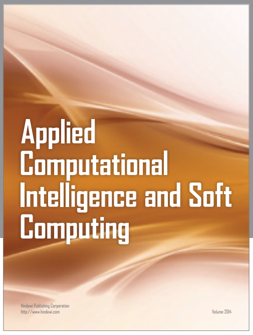
[41] H. Yan, D.A. Maltz, T.S. Eugene Ng et al., Tesseract: A 4D Network Control Plane, In *Proceedings of USENIX Symposium on Networked Systems Design and Implementation* (*NSDI 07*), April 2007.

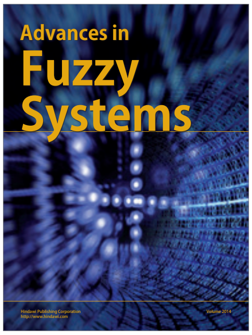

Advances in
Multimedia

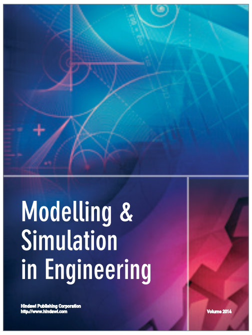
The Scientific World Journal

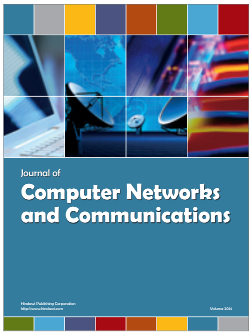

International Journal of
Distributed Sensor Networks

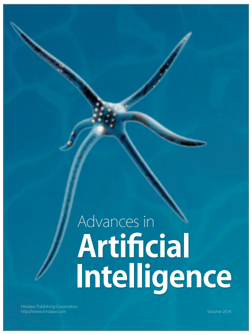

Journal of
Industrial Engineering

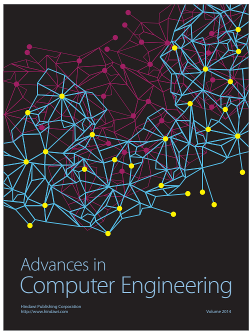

Applied Computational Intelligence and Soft Computing


Advances in
Fuzzy Systems

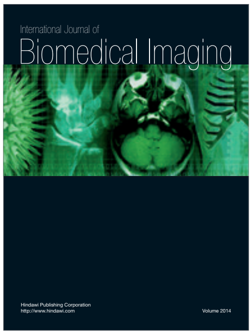

Modelling & Simulation in Engineering

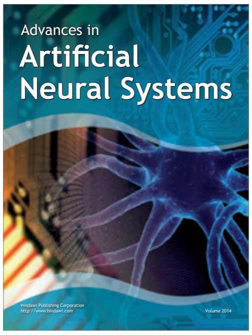

Journal of
Computer Networks and Communications

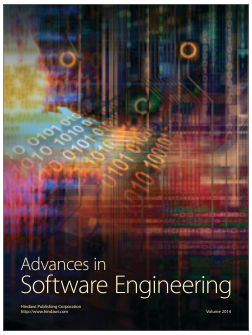

Advances in
Artificial Intelligence


Advances in
Computer Engineering

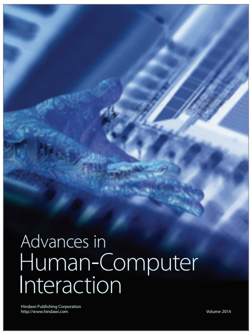
International Journal of
Computer Games Technology

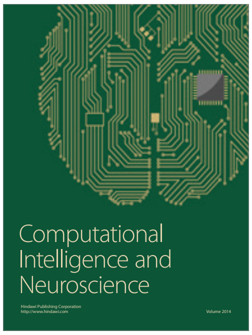

International Journal of
Biomedical Imaging


Advances in
Artificial Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer Interaction


Computational Intelligence and Neuroscience

International Journal of
Reconfigurable Computing

Journal of
Electrical and Computer Engineering