GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

TO SECURE INTEGRATION OF HETEROGENEOUS ADVANCED WIRELESS NETWORKS (SHAWK) FOR UBIQUITOUS INTERNET ACCESS

G.PRAVEENA
Department of computer science and Engineering Bharathidasan University, India

ABSTRACT

A **heterogeneous network** is a network that connecting computers and other devices with different operating systems and/or protocols. For example, the local area networks (LANs) that connect Microsoft Windows and Linux based personal computers with Apple Macintosh computers are heterogeneous.[1][2] The word **heterogeneous network** is also used in wireless networks using different access technologies. For example, a wireless network which provides a service through a wireless LAN and is able to maintain the service when switching to a cellular network is called a wireless heterogeneous network. To balance between the security and performance requirements in such heterogeneous networks from MAC layer to application layer, including a customized context-aware media independent handoff (MIH) framework, a unified access tested for 4G and Wi-Fi integration, a secure fast handoff scheme between different wireless networks, a practical secure routing solution to defend wormhole attack and an novel application for secure application mobility.

Keywords—Heterogeneous wireless networks, Context-aware MIH, Unified access, Seamless handoff.

I. INRODUCTION

In this article, we are witnessing the development and deployment of a large number of wireless networking technologies including 3G, WLANs, Bluetooth, and Ultra wideband. At the same time we are seeing a convergence of core networking infrastructure on the Internet Protocol Suite (IP) [5]. IPv4 is widely deployed throughout the Internet and there is now a serious attempt to deploy IPv6, which offers a much large IP address space (128bits) as well as easier protocol processing and mobility enhancements. Looking at this from an OSI perspective, Layers 1 and 2 are being hugely expanded in the wireless domain with Layer 3, the network layer, becoming fixed on IP. The result is that IP must support key features associated with wireless networking including handover, location, and mobility management. Moreover, due to the multiplicity of choices available from many cellular/wireless network providers, different access technologies, and disparate application's QoS requirements, there is a significant need to come up with a single unified approach. The 4G architecture envisions highly flexible and adaptive integration of diverse mobile client systems and network technologies to support built-in capability for seamless wireless access. Implicitly, this also means that there will be a need for mobile devices that can cope with the complexity and dynamics of next generation (4G) wireless access environments. With more technologies, services, and

devices joining the fray, we can expect that the gap between the service levels offered by new access networks will close, adding more complexity to the handover process Mobile IP has been developed to support mobility.

II. HANDOVER MECHANISMS

Handover introduces packet loss and latency which can severely damage data communication. TCP, part of the IP Suite and used throughout the Internet, reacts extremely adversely to packet loss. This is because TCP assumes all packet loss is due to congestion and limits its window-size as a result, leading to reduced performance. Multimedia applications which normally have strict temporal constraints can be also affected by increased latency.

III. ROUTING PROTOCOLS FOR MANETS

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network.

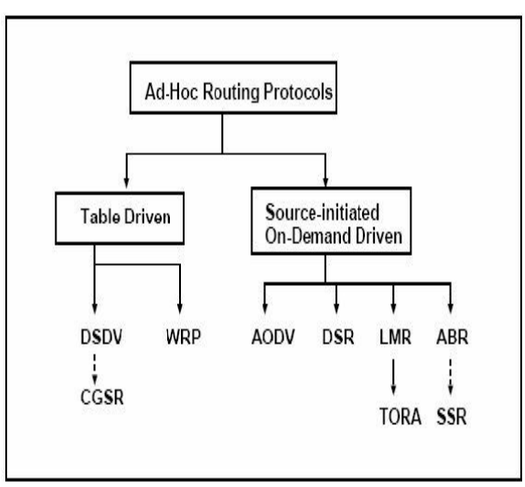


Fig.1 routing protocols for manets

A. **Table-Driven Routing Protocols**

1) Destination-Sequenced Distance-Vector Routing (DSDV)

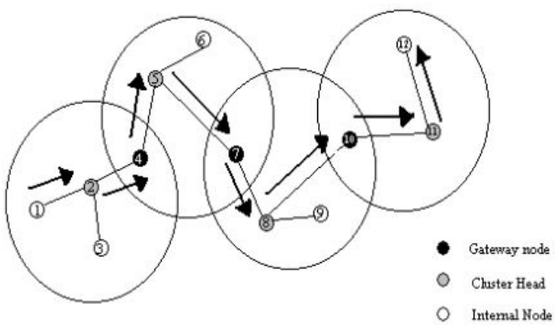
Destination-Sequenced Distance-Vector Routing protocol is

a proactive table driven algorithm based on classic Bellman-Ford routing. In proactive protocols, all nodes learn the network topology before a forward request comes in. In DSDV protocol each node maintains routing information for all known destinations. The routing information is updated periodically. Each node maintains a table, which contains information for all available destinations, the next node to reach the destination, number of hops to reach the destination and sequence number. The nodes periodically send this table to all neighbors to maintain the topology, which adds to the network overhead. Each entry in the routing table is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops [9].

2) Cluster head Gateway Switch Routing (CGSR)

Uses DSDV as an underlying protocol and Least Cluster Change (LCC) clustering algorithm. A cluster head is able to control a group of ad-hoc hosts. Each node maintains 2 tables: A cluster member table, containing the cluster head for each destination node. A DV-routing table, containing the next hop to the destination. The routing principle: Lookup of the cluster head of the destination node, Lookup of next hop, Packet send to destination, Destination cluster head delivers packet.

Drawbacks is too frequent cluster head selection can be an overhead and cluster nodes and Gateway can be a bottleneck .



3) The Wireless Routing Protocol (WRP)

Table-based protocol with the goal of maintaining routing information among all nodes in the network.Each node is responsible for four tables: Distance table,Routing table,Link-cost table, Message retransmission list (MRL) table.Link exchanges are propagated using update messages sent between neighboring nodes., Hello messages are periodically exchanged between neighbors. This protocol avoids count-to-infinity problem by forcing each node to check predecessor information. Drawbacks: 4 tables requires a large amount of memory and periodic hello message consumes power and bandwidth .

Source-Initiated On-Demand Routing Protocols

1) Ad-Hoc On-Demand Distance Vector Routing (AODV)

Builds on DSDV algorithm and the improvement is on minimizing the number of required broadcasts by creating routes on an on-demand basis (not maintaining a complete list of routes).Broadcast is used for route request. Advantages: uses bandwidth efficiently, is responsive to changes in topology, is scalable and ensures loop free routing. Drawbacks: nodes use the routing caches to reply to route queries. Result: "uncontrolled" replies and repetitive updates in hosts' caches yet early queries cannot stop the propagation of all query messages which are flooded all over the network.

2) *Dynamic Source Routing (DSR)*

Based on the concept of source routing. Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware2 major phases: Route discovery – uses route request and route reply packets Route maintenance – uses route error packets and acknowledgments .Advantages: No periodic hello message and fast recovery - cache can store multiple paths to a destination Drawbacks: the packets may be forwarded along stale cached routes. It has a major scalability problem due to the nature of source routing. Same as AODV, nodes use the routing caches to reply to route queries.

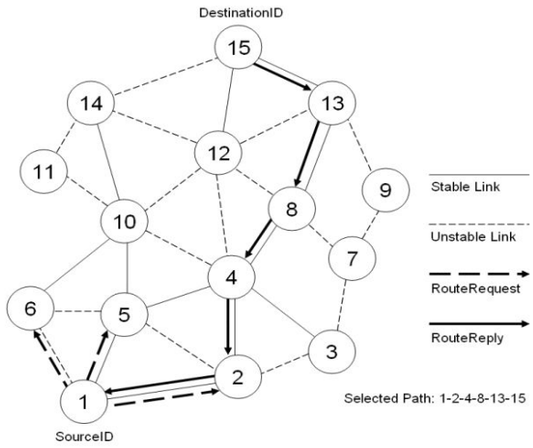
3) *Temporally-Ordered Routing Algorithm (TORA)*

Highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal.Proposed to operate in a highly dynamic mobile networking environment.It is source initiated and provides multiple routes for any desired source/ destination pair.This algorithm requires the need for synchronized clocks.3 basic functions: Route creation, Route maintenance, Route erasure. Advantages: provides loop free paths at all instants and multiple routes so that if one path is

not available, other is readily available. It establishes routes quickly so that they may be used before the topology changes. Drawbacks: exhibits instability behavior similar to "count-to-infinity" problem in distance vector routing protocols.

4) Associatively-Based Routing (ABR)

Free from loops, deadlock, and packet duplicates, and defines a new routing metric for ad-hoc mobile networks. Each node generates periodic beacons (hello messages) to signify its existence to the neighbors. These beacons are used to update the associativity table of each node. With the temporal stability and the associativity table the nodes are able to classify each neighbor link as stable or unstable.ABR consists of 3 phases: Route Discovery, Route Repair/Reconstruction, Route Delete .If node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started.



Advantages: free from duplicate packets. Drawbacks: Short beaconing interval to reflect association degree precisely.

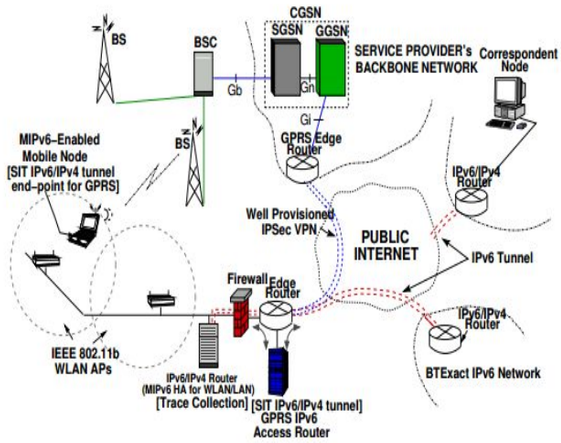
5) Signal Stability Routing (SSR)

It is a descendent of ABR and ABR predates SSRit selects routes based on signal strength between nodes and on a node's location stability thus offers little novelty.SSR route selection criteria has effect of choosing routes that have 'stronger' connectivity and it can be divided into: Dynamic Routing Protocol (DRP) or Static Routing Protocol (SRP).DRP is responsible for maintenance of signal stability table and routing table .SRP processes packets by passing the packets up the stack if it is the intended receiver and forwarding the packet if it is not Advantages: to select strong connection leads to fewer route reconstruction. Drawbacks: long delay since intermediate nodes can't answer the path (unlike AODV, DSR).

6) Testbed

To closely emulate the next generation (4G) integrated networking environment, our experimental testbed setup consists of a tightly-integrated, Mobile IPv6-based GPRS-The cellular GPRS network infrastructure currently in use is the Vodafone UK's production GPRS network.

The WLAN access points (APs) are IEEE 802.11b APs. Our testbed has been operational since March 2003, and results showing how we optimise vertical handovers are detailed in [3].



In the testbed, the GPRS infrastructure comprises base stations (BSs) that are linked to the SGSN (Serving GPRS Support Node) which is then connected to a GGSN (Gateway GPRS Support node). In the current Vodafone configuration, both SGSN and GGSN node are co-located in a single CGSN (Combined GPRS Support Node). A well provisioned virtual private network (VPN) connects the Lab network to that of the

Vodafone's backbone via an IPSec tunnel over the public Internet. A separate "operator-type" RADIUS server is provisioned to authenticate GPRS mobile users/terminals and also assign IP addresses.

For access to the 4G integrated network, mobile nodes (e.g., laptops) connect to the local WLAN network and also simultaneously to GPRS via a Phone/PCcard modem. The mobile node's MIPv6 implementation is based on that developed by the MediaPoli project [8], chosen for its completeness and open source nature. We brokered a semi-permanent IPv6 subnet from BTExact's IPv6 Network, which connects us to the 6BONE. Using the address space, we are able to allocate static IPv6 addresses to all our IPv6 enabled mobile nodes. A router in the lab acts an IPv6/IPv4 tunnel end-point to the BTExact's IPv6 network. This router is also There is an IPv6 access router (Home Agent) for the lab's fixed-internal IPv6-enabled network and also for internal

WLANs (shown in Figure 3). Routing in the Lab has been configured such that all GPRS/WLAN user traffic going to and from mobile nodes are allowed to pass through the internal router, enabling us to perform traffic monitoring.

IV. SEAMLESS HANDOFF

Seamless handoff provides end-to-end IP continuity without failures in the midst of a download activity due to link outages or handovers. What this means is that a user or application that is connected to a handoff server could seamlessly and transparently switch back and forth between different internet technologies, without compromising any communication activity. Seamless handoff ensures successful data transfer even when the underlying link connections are damaged or disrupted due to device mobility. Furthermore, it guarantees this lossless Quality-of-Service when a mobile user or application passes through different alternative technologies.

Seamless Handoff Applications

Seamless handoff can be used in a variety of applications. For example, many consumers now are able to purchase internet-enabled cellular phones and similar handheld devices. These devices can be used to transfer video, audio, and other large delay sensitive types of media. With seamless handoff, the quality of transmission improves considerably. Music delivery over cellular networks is also possible [2]. A wireless entry point to music delivery networks (e.g. wireless music portals) may represent an innovative and value-added service offered by cellular carriers to those mobile customers wishing to use their 2.5/3G enabled cellular phones for playing out songs, as well as other multimedia objects [2]. There are many areas where seamless handoff can be applied, with emphasis in mobile applications that are delay sensitive, run in real-time and must be connected to the internet constantly.

Goals of Seamless Handoff

The goals of seamless handoff are the following:

- Continuous connectivity
- Low latency
- Minimum packet loss
- Minimum infrastructural modifications

Handoff Diagrams

The following are some diagrams that provide a high-level view of the seamless handoff architecture and the various scenarios that can be used with it.

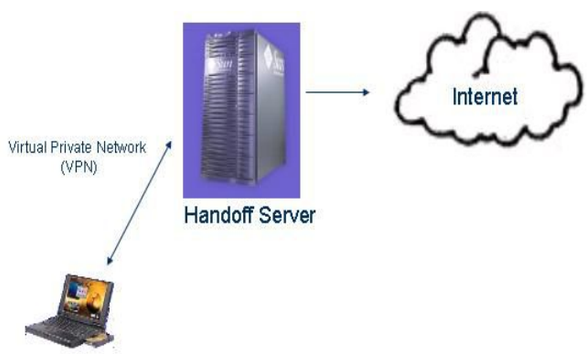


Figure 2: Laptop using a Handoff Server as an access point

In Figure 2, a laptop is connected to a handoff server using a virtual private network (VPN) connection. The handoff server maintains the internet connection, and will be responsible for providing the laptop with both horizontal and vertical handoffs should the need arise.

In Figure 3, a PDA is connected via a Bluetooth adapter to the laptop. The laptop is connected to a handoff server using a virtual private network (VPN) connection. The handoff server maintains the internet connection, and will be responsible for providing the laptop with both horizontal and vertical handoffs should the need arise.

It can be seen that numerous chaining possibilities are possible in the seamless handoff architecture. The architecture is very flexible since the handoff server provides a centralized architecture where connecting clients can connect in an ad-hoc manner.

Figure 3: PDA connected to a Laptop via Bluetooth

Secure application mobility: To enable the secure application

mobility, the requirement of security context transfer (SCT)

protocol during the device handover was previously introduced in [27], [28]. The early works [29], [30] have specified security. requirements for SCT on handover. Based on these works, [31]

Further presents a thorough threat analysis of security solutions that are based on security-context transfers during interprovider handover. The main advantage of [35] is that it allows mobile devices and networks to express policies with respect to whether or not a handover should take place, dependent on the history of previously used security mechanisms that is included in the security-context transfer.

V. CONCLUSION

In this paper, we investigated the challenging issues for Secure integration of heterogeneous wireless networks for

ubiquitous Internet access. We developed and implemented practical mechanisms to ensure the security guarantee and meet the performance requirements in our SHAWK platform. These mechanisms can effectively improve security of the heterogeneous wireless networks, with minimal network architecture modification.

REFERENCES

[1] S. Aust, D. Proetel, N. A. Fikouras, C. Pampu, and C. Gorg. Policy based Mobile IP handoff decision (POLIMAND)

using generic link layer information. In Proceedings of 5th IEEE International Conference on Mobile

and Wireless Communication Networks (MWCN 2003), October 2003.

[2] A. Campbell, J. Gomez, C.-Y. Wan, S. Kim, Z. Turanyi, and A. Valko. Cellular ip. Internet Draft (draft-ietfmobileip-

cellularip-00.txt), , Work in Progress, January 2000.

[3] R. Chackravorty, P. Vidales, I. Pratt, and J. Crowcroft. On TCP Performance during Vertical Handovers: Experiences

from GPRS-WLAN Integration. In Proceedings of The Second IEEE International Conference on Pervasive

Computing and Communications (PerCom'04), March 2004.

[4] Daedalus wireless research group. http://daedalu.cs.berkeley.edu/.

[5] ISI-USC. Transmission Control Protocol and Internet Protocol speci_cations, IETF RFC 791 and IETF RFC 793,

1981.

[6] D. B. Johnson, C. E. Perkins, and J. Arkko. Mobility Support in IPv6 (RFC 3775) http://www.ieft.org,

2004.