# Heterogenous Networks Architectures and Their Security Weaknesses

Samad Baseer

***Abstract*—In recent years the wireless communication networks combined with the wired networks have made tremendous progress with both the upgrade of cellular networks to support wide area data access and the widespread deployment of IEEE 802.11 based local area networks. Although both wired and wireless provides advantages and disadvantages in their own unique way it is the integration of these networks that we can reap the real technological reward from both. Although there is extensive research ongoing on individual networks in isolation it is the combination of these networks where the information highway will be open to all and in this case the need for architecture that fulfills the demands of the users in all scenarios. The various heterogeneous wireless networks architectures proposed are Unified Cellular Ad hoc Network (UCAN), (Integrated Cellular Ad hoc Relay (iCAR) and Scalable Proxy Routing (SPR) and multiple hop cellular networks. Although each has their unique design and protocol we discuss them and also point out their security weaknesses in any attack.**

***Index Terms*—Heterogeneous networks, UCAN, iCAR, SPR, security weaknesses.**

## I. Introduction

Diversity and Complexity are the titles of the coming communication technologies. This situation caused by the increased production of the communication devices and systems without depending on one standardized concepts or common language. Most of the systems and devices nowadays concern on heterogeneous networks. That raised the intensive need to find one station to control and manage these networks since controlling them separately brings a lot of difficulties and inconsistency. Heterogeneous networks will be enabling to support many services and applications in heterogeneous networks such as multimedia applications.

The capacity of a cellular data network can be improved by creating a larger number of smaller cells, each of which houses an expensive base-station (BS). The benefit of such an approach is the increased spatial reuse of the spectrum. Alternatively, in order to increase spatial reuse, cellular networks may be augmented with ad-hoc wireless connectivity; this is attractive as compared to the former approach in terms of the incurred cost [1], [2]. We call these latter types of networks hybrid cellular-ad hoc networks or simply heterogeneous networks. Such a network can be shown in Fig. 1.

Manuscript received August 6 2012; revised September 29, 2012.

Samad Baseer is with the Software Engineering Department of the KPK University of Engineering and Technology Peshawar (e-mail: samadbaseerkhan@gmail.com)

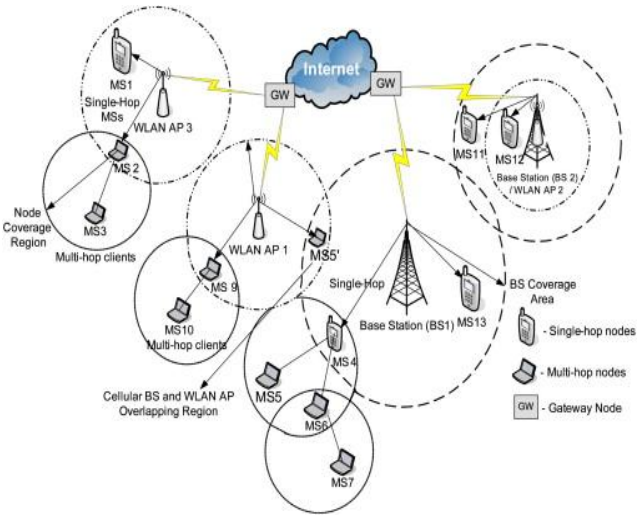



Fig. 1. Futuristic heterogeneous multihop wireless architecture [3].

The designs of the future wireless networks will have to put a huge effort on the security and trust management. The main reason for this is that future networks will be decentralized and ad hoc in nature and hence allowing various types of network mobile terminals to join and leave. All the nodes are free to move and dynamically connect in any arbitrary manner. The establishment, maintenance, and operation of this kind of networks rely on cooperation among nodes, which must handle the necessary networking tasks acting as routers and hosts. In particular far off nodes communicate using intermediate nodes as relays, through routes that nodes themselves discover and maintain. [4].

In the wireless networking environment majority of the networking functions must be performed by the nodes themselves. Due to lack of routing infrastructure they have to cooperate to communicate. Nodes are rational their actions are strictly determined by self interest. Therefore misbehavior exists. Malicious nodes are the nodes that join the network with the intent of harming it by causing network partitions , denial of service, etc. while selfish nodes that utilize services provided by others but do not reciprocate to preserve resources. Thus in order to save battery and bandwidth nodes should not forward packets for others. [5].

Unlike nodes of conventional wireline networks nodes of wireless networks cannot be assumed to be secured in locked cabinets. Therefore they risk being captured and compromised. As all communications are performed over the air wireless networks are vulnerable to attacks ranging from denial of service to eavesdropping. This makes the entire network vulnerable and very sensitive to attacks. Because of the broadcast nature of the wireless transmission anyone within communication range can intercept the data that was not intended to them.

In such a complex environment the current cryptographic methods with high level security may not work. Ad hoc and cellular networks have received a great attention in recent years. To accommodate the large number of users and traffic over a large geographic area, cellular networks could take advantage of the infrastructure less ad hoc networks to provide extended service. One of the key issues in the integration of cellular and ad hoc networks is to find some mobile nodes who would act as proxies or relays. These proxies or relays will forward the information to the mobile nodes placed far away from the base station (BS). Much architecture has been proposed to understand and in future implement the design for successful data delivery. Although the architectures have focused on the increase of system capacity, coverage of cellular networks and improving the throughput of the whole network system. The terminals with dual access interfaces could act as relay nodes to route the data. Those nodes could have a wider bandwidth up to 11Mbps while 802.11a offers bandwidth up to 54Mbps **[6]**. None of the work to the author's knowledge has discussed the impact of security of these networks. Our work is an analysis of the existing architectures of the heterogeneous networks and how they would react to the attack scenario.

## II. Wireless Security Measures

There are many issues in the Heterogeneous networks where only the most important issues discussed are Handoff issues and throughput and delay and how to maintain QoS when the networks are changed. Limited architecture considers the work of a security protocol in their mechanisms and considers all the nodes to be trustworthy and reliable. The main insecurity with wireless networks compared to wired networks is the easy of accessing the transmission medium used, i.e. with a wired network to sniff packets, there has to be a physical access to the network whilst with wireless networks, the transmission is easily available outside the physical building. Insecurities on wireless networks other than those caused by the ease of accessing the transmission media are the same as for a wired network, i.e. packets can be sniffed if sent in clear text across wires if someone has packet sniffing software on the same segment of the network as the packet is being transmitted across.

## III. Unified Cellular and AdHoc Routing

The fundamental aspect of wireless communication is its broadcast nature i.e. transmission from a node can be overheard at several locations. This makes wireless communication inherently vulnerable to eavesdropping by an adversary. As the use of wireless networks grows the security aspects have yet to be controlled. These issues have been identified by recent discoveries that the wireless networks are vulnerable to eavesdropping. Thus a fundamental question is how to ensure secrecy in wireless networks. Although there has been extensive research in both Cellular layout and Mobile AdHoc Networks to date, on improving the performance of each of these two technologies in isolation, one question that remains is whether they can be synergistically combined to leverage the advantages of each other. UCAN is a new wireless networking paradigm that increases the throughput of wide-area wireless networks through opportunistic use of ad hoc local-area wireless networks. The architecture of UCAN can be shown in Fig. 2.

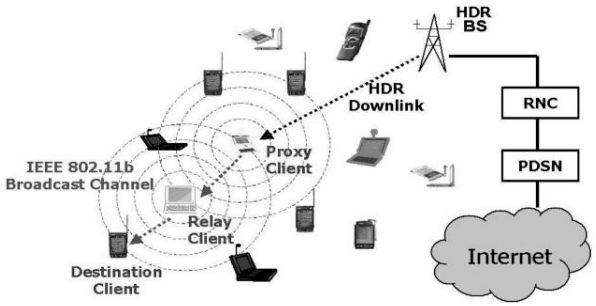



Fig. 2. UCAN architecture [12].

One prerequisite for the UCAN model is that each mobile device is equipped with two wireless interfaces. Fortunately, given the popularity of the IEEE 802.11b (Wi-Fi) interface, it is already being embedded in every mobile device and, thus, the device only needs a 3G interface card to operate in UCAN. The convergence of mobile phones and computers, such as walkie-talkie PC, also foresees the popularity of such wireless devices. More recently, several companies, such as GTRAN wireless, are offering integrated cards that implement both IEEE 802.11b and 3G wireless interfaces. Thus, if routing protocols can be made aware of both interfaces, they can improve performance significantly by selecting the best interface(s) to deliver packets to the mobile users. [7]

In UCAN the AdHoc routing component is much more efficient and reliable because of its explicit use of the cellular infrastructure and the protocol complexity is also significantly lower. This method is broken down into two methods i.e. greedy proxy discovery and also on demand proxy discovery. Both of these methods are explained.

### *A. Greedy Proxy Discovery Method*

In greedy proxy discovery, neighboring mobile clients within the one-hop IEEE 802.11b transmission range periodically exchange their average downlink channel rates by broadcasting a neighborhood advertisement message (NBADV). Thus, each mobile client proactively maintains a table of its neighbors' IDs (e.g., IP addresses) and their most recently advertised average high data rate (HDR) downlink channel rates. The destination client also sets its fields of its NBADV packet so that only those clients within a certain range from the destination client need to establish neighborhood information.

### *B. On Demand Proxy Discovery*

In on-demand proxy discovery, mobile clients do not proactively maintain their neighborhood information. Instead, the destination client reactively floods a route request (RTREQ) message within a certain range. The RTREQ message carries the destination client's average HDR downlink channel rate and a sequence number that is incremented every time the destination client initiates a new round of proxy discovery.

## IV. Security Weaknesses

The UCAN architecture although a pioneer work in the field of heterogeneous networks , still fails to address any attack mechanisms it might have against the malicious nodes. As there are two types of attacks malicious and selfish the methodology fails to pinpoint any one of them

The problem in UCAN is flooding messages and inefficient relay proxy. As there are more and more users joining and leaving the cell or network thus keeping records of each one is very difficult to maintain. If this protocol is implemented then the delay between nodes and delivery ratio is increased.

This also shows no strategy to provide as to how to defend from any such attack. This architecture is most prone to denial of service attack where a node can be attacked and it would be used to send more and more packets to other nodes and thus the whole network is failure prone. As any mobile node can exchange wrong information about its MAC address and thus cheat other nodes to send it data.

## V. Integrated Cellular AdHoc Routing (iCAR)

The *iCAR* system is a representative heterogeneous wireless system, proposed to address the congestion problem in the wireless networks. *iCAR* system [8], [9], has been proposed to deploy the AdHoc networking technology in the cellular system to address the congestion problems due to limited wireless bandwidth and dynamically varying traffic load. By using the *Ad hoc Relaying Stations (ARSs)* along with the signaling and routing protocols presented by [10] it is possible to divert traffic from one (possibly congested) cell to another (non-congested) cell. iCAR, with its ability to leverage both the cellular and ad hoc relaying techniques to increase system's capacity, is a promising evolution path to the next generation heterogeneous system. In [9], [11], the performance of iCAR in terms of the call blocking probability has been studied via analysis and simulations. It has been shown that iCAR can effectively balance traffic load among cells, and more importantly, overcome the barriers imposed by the cell boundaries and share channels between cells, which in turn leads to significantly lower call blocking probability than a corresponding cellular system can achieve. Recent studies on hand-off performance in iCAR [12], [7], [11] has shown that with the same amount of resource as in conventional cellular systems and a limited number of ARS's, the iCAR system can reduce hand-off call dropping probability significantly and achieve higher channel efficiency. The layout of iCAR is shown in Fig. 3.

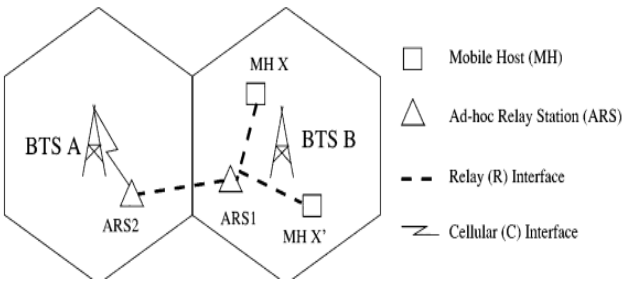



Fig. 3. A relaying example where MH X communicates with BTS through two ARSs [5].

## VI. Security Shortcommings

However the authors primarily focus on improving the cell blocking probability for circuit like traffic by diverting traffic from congested cells to neighboring lightly loaded cells or cold cells. They use redeployed dedicated stationary relays for this purpose resulting in increased cost.

This methodology is using only the (ARS's) for more cellular coverage capacity but it does not show how the integration process will be carried out i.e. the process of building and involving more and more mobile ad hoc network users into the system. So thus its overall system is not that much secure. It tries to focus on more of the security policies that are placed in the cellular technology and have a link with the mobile station center where it can gather the required information for forwarding data packets. The method does not consider even one security risk and it is not the case in real world where other nodes may be malicious or selfish or misbehaving.

## VII. Scalable Proxy Routing (SPR)

A Scalable Proxy Relay Routing Protocol (SRP) is used to increase the total throughput of the system. In this strategy, the base station always sends data to the destination node through the selected proxy nodes which has minimum transmission delay. The selection of the relay should be such that it has the minimum delay. This protocol is different from the other protocols in the sense that none of them have considered the transmission delay from a mobile node to the base station. Currently, most cellular network employs digital technology to improve the system quality and services. Typical present cellular networks include GSM, GPRS, CDMA, WCDMA, etc. Wireless Ad-hoc network is a temporary wireless mobile network which is organized by a collection of wireless mobile devices without the aid of any established infrastructure [6], [13], [14]. The layout of SPR is shown in Fig. 4.

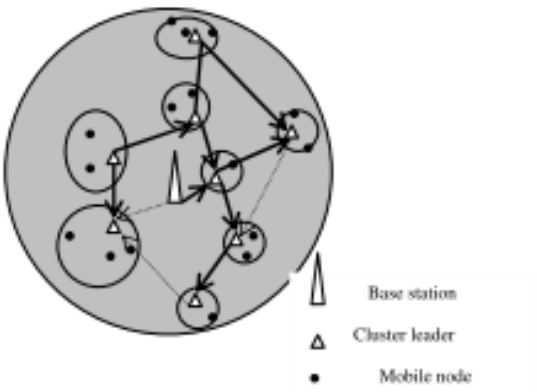



Fig. 4. Shortest path from base station to cluster leaders [1].

## VIII. Security Flaws

As we know the more hops there are, the larger the delays and the more chances of corruption and attacks are increased. Thus both Quality of Service (QoS) and security of the whole system can be affected. This protocol not only increases the whole system throughput but also reduces the delay by

selecting the shortest path from a base station to the selected cluster leader which further relays the message to the destination nodes. This method also keeps updated about the nodes as to who is having the best delay to the destination and path to the destination. As this is a scenario of mobile ad hoc networks so mobile nodes are joining and leaving all the time thus you have to maintain the tables and also update the table after so many transactions.

This method does not provide any incentive as to why the mobile nodes should forward data information or packets to any other node and waste its limited battery power while he himself has no concern for the data of other user.

A lot of processing is also done in selecting the cluster header the reason being that in mobile Ad Hoc networks nodes can leave and join anytime. So a lot of computation power will be wasted in sending updated information and receiving information thus a lot of messages are being sent and received and thus computation ability will also make the response slower.

A close analysis of the protocol shows that this is not an efficient secure protocol for the heterogeneous networks the reasons being that there is no security mechanism installed at all. It takes the scenario that two different networks are combined namely cellular and mobile ad hoc networks and the shortest delay path to the destination is chosen from a cluster head. What the authors have not mentioned is that suppose that a node gets malicious and shows that it is having the smallest delays to the destination thus it will be chosen as the cluster leader even though that the information shared is all false .

Thus it can attack *k* other nodes and thus valuable data will be lost and no method exists in this scheme to find out how to remove or fix the problem. Thus this protocol is very much prone to wormhole Sybil and blackhole attacks. The Sybil attacks can also be used to get the other nodes trust. Thus it would be declared a cluster leader and if colludes with the other malicious nodes then serious damage can be done to the system. This method has no cure for removing the malicious nodes. Thus from a security point of view this is a very weak protocol and can be breached very easily from the mobile ad hoc networks side.

## IX. Conclusions

Various new protocols are being introduced for the heterogeneous networks. The research trend is to handle more multimedia traffic without any delays. We want an increase in system capacity, throughput. While at the same time no attention is being paid to the security architecture of the protocol. What effects will an attack have on the system capacity or how it will respond? Our forthcoming work will focus on showing how an attack can damage the system capacity and show its effects on throughput and delivery ratio.

## References


[1] B. Liu, Z. Liu, and D. Towsley, "On the capacity of hybrid wireless networks," in *IEEE Infocom*, 2003, pp. 1543–1552.

[2] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "UCAN: A unified cellular and Ad-Hoc network architecture," in *ACM Mobicom*, 2003.

[3] A. George, A Kumar, D. Cavalcanti, D. P. Agarwal, "Protocols for mobility management in heterogeneous multihop wireless networks," *International Journal of Pervasive and Mobile Computing* vol. 4, pp. 92-116 , 2008

[4] M. Conti, E. Gregori, and G. Maselli, "Reliable and efficient forwarding in Ad-Hoc networks," *International Journal of Ad-Hoc Networks* vol. 4, no. 3, 2006

[5] K. Wang, M. Wu, and S. Shen, "A trust evaluation method for node cooperation in mobile Ad-Hoc networks," *Fifth International Conference on Information Technology Next Generations IEEE Computer Society*, 2008

[6] Yang and G. Fan, "Scalable proxy routing in multi-hop cellular networks," *Springer Verlag Berlin Heidelberg* 2006

[7] H. Wu, S. De, C. Qiao, E. Yanmaz, and O. Tonguz, "Hand-off performance of the integrated cellular and ad hoc relaying (icar) system," 2002.

[8] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated cellular and Ad-Hoc relaying systems: iCAR," *IEEE J. Selected Areas in Comm.*,vol. 19, no. 10, pp. 2105-2115, Oct. 2001.

[9] H. Wu, S. De, C. Qiao, E. Yanmaz, and O. Tonguz, "Queuing delay performance of the integrated cellular and Ad-hoc relaying system," *IEEE* 2003

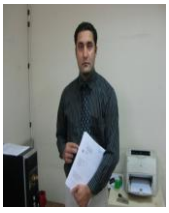
[10] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated cellular and Ad-Hoc relay systems: iCAR," *IEEE Journal on Selected Areas in Communications special issue on Mobility and Resource Management in Next Generation Wireless System*, vol. 19, no. 10, October. 2001.

[11] H. Wu and C. Qiao, "Modeling iCAR via multi-dimensional markov chains," *ACM Mobile Networking and Applications (MONET), Special Issue on Performance Evaluation of Qos Architectures in Mobile Networks*, 2002

[12] H. Wu, C. Qiao, and S. Dixit, "Signaling and routing protocols in icar (integrated cellular and ad hoc relaying system)," in *Wireless IP*, ch. 21, Artech House, 2002

[13] S. Lee, S. Banerjee, and B. Bhattacharjee,"The case for a multi hops wireless local area network," in *Proceedings of IEEE INFO-COM*, 2004.

[14] S. Radhakrishnan, G. Racherla, C. Sekharan, N. Rao, and S. Batsell, "Protocol for dynamic Ad-Hoc networks using distributed spanning trees," *Wireless Networks*, vol. 9, pp. 673-686, 2003.

**Engr. Samad Baseer** completed his B.Sc. and M.Sc in Computer Systems Engineering from University of Engineering and Technology Peshawar Pakistan. Currently, he is enrolled as a PhD candidate at Asian Institute of Technology, Thailand. His field of study is Information and Communications Technologies. He is employed as Senior Lecturer in the Department of Computer Software Engineering Department Mardan Campus University of Engineering and Technology Peshawar. His research interests include Cooperative Communications, Security Issues in Heterogeneous Networks, Cross Layer approach for Multimedia applications. Mesh and Sensor Networks Reliability and Security Issues.