

SECURE 3G USER AUTHENTICATION
IN AD-HOC SERVING NETWORKS

A Thesis
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
requirements for the degree of
Master of Science of Systems Science
in

The Department of Computer Science

by
Lyn L. Evans
B. S., Louisiana State University, 1989
December 2005

Table of Contents

Abstract.....	iii
Introduction.....	1
Merging 3G and Wireless IP Networks.....	2
3G Network Architecture.....	3
802.11 Wireless LAN Architecture.....	4
3G-WLAN Integrated Architecture.....	6
3G Security Architecture.....	9
802.11 WLAN Security.....	13
3G-WLAN Security Architecture.....	15
Risk Analysis of 3GPP-WLAN Security.....	18
Enhanced EAP-AKA Security Protocol.....	20
Authentication Control in EAP-AKA Protocol.....	20
Spatial Control in EAP-AKA Protocol.....	20
Risks of Spatial Control in EAP-AKA Protocol.....	22
Securing 3G-WLAN User Authentication.....	24
3G-WLAN Trust Model.....	24
Benefits of Ad-Hoc Serving Networks.....	25
3G and Ad-Hoc WLAN Security Procedures.....	26
Authentication Acknowledgement.....	26
Determining Trust in Serving Networks.....	28
Protecting 3G Network Services.....	33
Conclusion.....	35
References.....	36
Vita.....	38

Abstract

The convergence of cellular and IP technologies has pushed the integration of 3G and WLAN networks to the forefront. With 3G networks' failure to deliver feasible bandwidth to the customer and the emerging popularity, ease of use and high throughput of 802.11 WLANs, integrating secure access to 3G services from WLANs has become a primary focus. 3G user authentication initiated from WLANs has been defined by an enhancement to the extensible authentication protocol, EAP, used to transport user authentication requests over WLANs. The EAP-AKA protocol executes the 3G USIM user challenge and response authentication process over the IP backbone for WLAN serving networks. To improve the degree of control of 3G subscribers, spatial control has been proposed for 3G-WLAN user authentication. Successful execution of 3G security algorithms can be limited to a specified area by encrypting a user's authentication challenge with spatial data defining his/her visited WLAN. With 3G networks' limited capacity to determine a user's location to the granularity of a small WLAN area and restricted access to users' location due to privacy, 3G operators must rely on spatial data sent from visited WLANs to implement control for authentication. The risks of implementing EAP-AKA spatial control by 3G operators with no prior relationship or trust for serving WLAN networks are presented in this paper. An ad-hoc architecture is proposed for serving networks in 3G-WLAN integration and the advantages of this architecture that facilitate secure 3G user authentication are identified. Algorithms are proposed to define robust trust relationships between the parties in 3G-WLAN networks. The security of 3G user authentication is further protected by new mechanisms defined that are based on the quality of trust established between parties.

Introduction

Mobility is an ubiquitous quality currently expected by voice and data cellular customers. Seamless mobility and services have been successfully integrated into cellular networks over the past decade, but there is an increased demand for richer services by mobile customers that is presenting new challenges to the cellular industry. This demand for enhanced services has sparked the convergence between cellular and IP networks as cellular services stand to be improved by utilizing the capacity of the IP backbone to deliver rich user data. The challenges presented by the convergence of these two networks are readily being addressed to facilitate the successful implementation of new mobile technology. Each network has been enhanced to provide both respective services, voice or data. Web data services have been integrated into 2G cellular networks with the introduction of the General Packet Radio Service, GPRS, and voice communications are now transported over IP networks using Voice-Over-IP encapsulation. These adapted data and voice services build the initial bridge between cellular and IP networks and deploy new technology layers for each respective network. IP and cellular networks differ fundamentally in infrastructure, communication protocols and properties and their convergence has become a technical research challenge. Designing hybrid cellular and IP access in integrated 3G and IP networks is the focus of this paper.

The services and technology provided by cellular and IP networks differ significantly. Voice communications are optimally carried over cellular networks which provide limited bandwidth and high security, while data is carried over an optical IP backbone providing powerful bandwidth and limited security. Second generation cellular networks currently provides 9.6 Kb/s, with 3G networks carrying 100 Kb/s. This limited bandwidth is efficient for voice transmission, but is a significant obstacle to carrying rich data services to cellular customers. Our current IP backbone carries more than 40 Gb/s and provides a future conduit for transporting data services to 3G customers. Challenges exist, however, in that security protocols in the respective IP and 3G networks are not compatible in architecture or in the quality of integrity and protection provided. Detailed analysis of the operational differences between the two network technologies is required to successfully define a secure, merged cellular and IP environment.

The most pending challenge of IP and cellular convergence is the secure and successful transport of 3G services over the IP backbone. Small wireless IP networks or WLANs are currently the most advantageous place to implement new merged cellular and IP access. Researchers have specified hybrid hardware to integrate 3G and WLAN networks as well as enhanced IP protocols to provide 3G network connectivity securely from IP WLANs. Relatively inexpensive deployment of hybrid WLANs providing access to 3G services will accelerate further convergence of IP and cellular networks. Gained access to enriched 3G cellular services from IP networks will become invaluable to customers and introduces new opportunities for technical advancement.

Merging 3G and Wireless IP Networks

Cellular operators have recognized the opportunity to offer high-speed data services to their customers through rapidly evolving WLAN technology. Global technical consortiums have been formed to address the technical requirements and define specifications for emerging 3G-WLAN integration. The 3rd generation partnership project, 3GPP, has defined 6 scenarios for integrating 3G and WLAN networks [3]. These scenarios defining potential integrated operation and services include:

- *Scenario 1* – Common billing and customer care for WLAN and 3G operators. In this scenario, the customer receives one billing statement listing both 3G and WLAN usage and can contact one customer service center concerning both services.
- *Scenario 2* – 3G access control and charging is used for traditional internet services over the 3G network through a WLAN. Customers are authenticated by the 3G core network without a separate procedure.
- *Scenario 3* – Customers access 3G packet-switched services over a WLAN. These services include short messages service SMS, multimedia message service MMS, and IP multimedia subsystem service IMS. Customers will simultaneously but independently access WLAN and 3G networks.
- *Scenario 4* – Customers can change access between 3G and WLAN networks during a service session. A session is re-established without user involvement and service interruption during switching is allowed.
- *Scenario 5* – Seamless service switching between 3G and WLAN sessions. The user should not experience significant interruption during a handover.
- *Scenario 6* – Customers access 3G circuit-switched services over a WLAN. Seamless service switching is implemented.

The scenario adopted by researchers for first stage 3G-WLAN deployment is *Scenario 3*. High-speed data services can be offered to customers with one subscription and one bill with limited or no change to the 3G network infrastructure. *Scenario 3* is a less expensive initial approach requiring a minimum of investment from cellular operators. The succeeding scenarios will require hybrid hardware designed to process both 3G and WLAN physical layer protocols in order to implement seamless roaming and circuit-switched services over WLANs. Implementing *Scenario 3* is currently pursued since existing IP protocols can be enhanced to deliver high-speed services and access 3G billing and authentication systems via the public packet data IP backbone.

The Broadband Radio Access Networks project, BRAN, within the European Telecommunications Standards Institute, ETSI, has additionally designed two options for internetworking GPRS, or the 2G packet service protocol over cellular networks, and WLAN networks [3]. These options define a *tight coupling* and *loose coupling* methodology for combined networking functionality.

- *Tight coupling* – Requires full 3G security architecture, protocol stacks and interfaces are implemented in a WLAN system. New adaptation functions or components would be present in user equipment and access points to transport GPRS signaling, or 2G packet services, over 802.11 WLANs networks. A 2G GPRS gateway would subsequently transfer

service requests onto the cellular network.

- *Loose coupling* – A WLAN is deployed as an access network complimentary to a GPRS network. A WLAN utilizes the subscriber databases in the GPRS network, but implements no data interfaces to the GPRS core network.

The most feasible option researched from the BRAN internetworking recommendations is the *loose coupling* design. Similar to the *Scenario 3* internetworking option defined by 3GPP, the public external packet network, or IP backbone, is accessed to perform 3G authentication and billing. *Loose coupling* offers a powerful advantage since new hardware communicating both GPRS and IEEE 802.11 protocols is not required. Defining enhanced, detailed access procedures for cellular customers accessing 3G services from a WLAN in a *loosely coupled* 3G and WLAN environment is the purpose of this paper.

3G Network Architecture

The infrastructure of future 3G networks has evolved from the Global System for Mobile Communication, GSM, standard that defines existing cellular networks. As several different international bodies initiated designing 3G standards, the 3rd Generation Partnership Program, 3GPP, was established to create common 3G standards and ensure interoperability between new emerging wireless networks [14]. The Universal Mobile Telecommunications System, UMTS, defined by ETSI, is also a synonymous term defining new 3G cellular networks. The fundamental difference between UMTS and the existing GSM network architecture includes the introduction of a new WCDMA air interface between the user equipment and 3G cell base stations. WCDMA brings critical enhancements to the previous 2nd generation CDMA system such as allowing frequency reuse at adjacent cells, less multipath interference, and higher security for transmitted signals [14]. Migration from GSM to new UMTS networks primarily involves implementing new protocols over the air interface between users and cell base stations for WCDMA. All aspects of 3rd generation cellular networks and services are address by technical groups within 3GPP to deliver multiple service types, including voice, video and data, seamless customer roaming and enhanced secure cellular architecture. The detailed specifications for delivering secure 3G service to WLAN networks defined by the WLAN/Cellular Internetworking team within 3GPP is the focus for this study.

3G network components are the User Equipment, UE, several Access Networks, AN, and a Core Network, CN. 3G user equipment connects with an access network over a radio air interface via a Base Transceiver Station or BTS. The area covered by a base transceiver station is defined as a 3G cell. The Access Network is comprised of a group of cells and their base transceiver stations which are managed by a Base Station Controller, BSC. The BSC provides the interface to the 3G core network which executes switching, routing and management processes for user applications and acts as a gateway to external networks. The core network provides access to centralized components and functions to maintain users' location data, build authentication and session keys for secure network use and maintain usage data for customer billing and charging. Authentication and session keys are built using a subscriber's secret key K_i which is stored within the Universal Subscriber Identity Module, USIM, inside the user

equipment. A user's secret key, K_i , is shared with the 3G core network and each user is identified by the 3G core network by his/her International Mobile Subscriber Identity, IMSI, which is also stored in the USIM.

Existing GSM networks were enhanced to service both *voice* and *data* user requests by adding access to *Packet Switched* services along with the original *voice Circuit Switched* services [14]. This enhanced GSM network employs the General Packet Radio Service to transport data over the user's air interface and allows access to simple data services such as Web access, or e-mail. The 3G core network required updating to transport *Packet Switched* services between user cells and a second distinct interface was added to the core network for access networks carrying GPRS services.

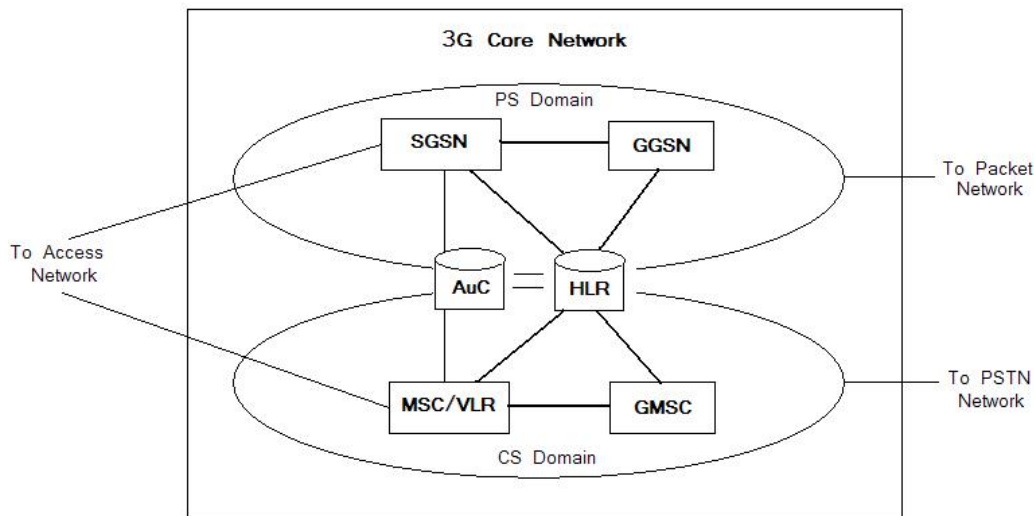


Figure 1 3G Core Network Components

Switching is accomplished in the core network for *circuit switched* connections by a Mobile Switching Center, MSC. For *packet switched* services, a Serving GPRS Support Node, SGSN, provides access to the 3G core network for users. Both entities access a Visitor Location Register to query current subscriber mobility and authentication data. The VLR accesses the 3G Home Location Register database containing the permanent identity of the user, IMSI, and the user's shared secret key for authentication. Connections between the 3G HLR and VLR are maintained to manage persistent services as the user moves throughout the network. The HLR maintains a mobile user's current MSC or SGSN association so to know where to route data packets or calls to users. A MSC also maintains access to a Gateway Mobile Switching Center, GMSC, which provides connectivity to external CS networks [14]. Access to external PS networks is provided by a Gateway GPRS Support Node, GGSN, which serves as a gateway for 3G users. The SGSN is unique from the MSC in that it performs routing of user data packets rather than voice calls and integrates the functionality of a VLR to maintain current subscriber information.

802.11 Wireless LAN Architecture

Traditional fixed IP networks have been extended to allow user mobility in small wireless local networks. With the implementation of IEEE 802.11 radio-based

communication standards, IP networking within small wireless areas allows mobile users to access data and applications hosted by fixed local servers. 802.11 WLANs also provide mobile users gateway access to external IP networks, primarily the public Internet. IP connectivity is implemented over a wireless area by use of dynamic IP addressing, or DHCP, which provided users a temporary IP address while they are accessing a WLAN. Both private and public WLANs have been implemented in which user authentication is required to gain network access or users access a WLAN as guests, respectively. WLAN Access Points, AP, transmit all IP packets between the WLAN user and application servers or gateways and allow users the freedom to move within the area covered by a WLAN. Simple, inexpensive WLANs have been integrated in popular facilities serving the public, such as airports or arenas, primarily to provide users with Internet access. This quick adoption of IEEE 802.11 WLAN technology has thus become a focal point for delivering converged 3G and IP network access.

A WLAN is comprised of several cells, similar to a 3G radio network, in which networking functions are accomplished by a fixed infrastructure or implemented by an ad-hoc architecture. With a fixed WLAN infrastructure, each cell is serviced by a Base Station, BS, or Access Point, AP. A network distribution system, typically Ethernet, connects all access points together and connects the WLAN to application servers and network gateways. Each cell is designated as a Basic Service Set by the 802.11 standard, while an entire WLAN, including all cells, access points, and distribution system is designated as an Extended Service Set [4]. Access point functionality is defined by the Distributed Coordination Function, DCF, which provides CSMA/CA access to wireless media equally between users. A Point Coordination Function is optionally implemented in WLAN access points to provide prioritized time-bounded services, such as voice or video. Power saving is implemented in user equipment employing an 802.11 interface allowing mobile stations to go into sleep mode while designated packets are buffered at the station's AP. Mobility management is accomplished in a WLAN as each user builds an association with his/her nearest access point serving the BSS in which she is located. Mobility becomes transparent in wireless LANs as users travel between cells and associate with different access points. Seamless connectivity is maintained without any disruption for ongoing user sessions. WLANs implementing an ad-hoc architecture do

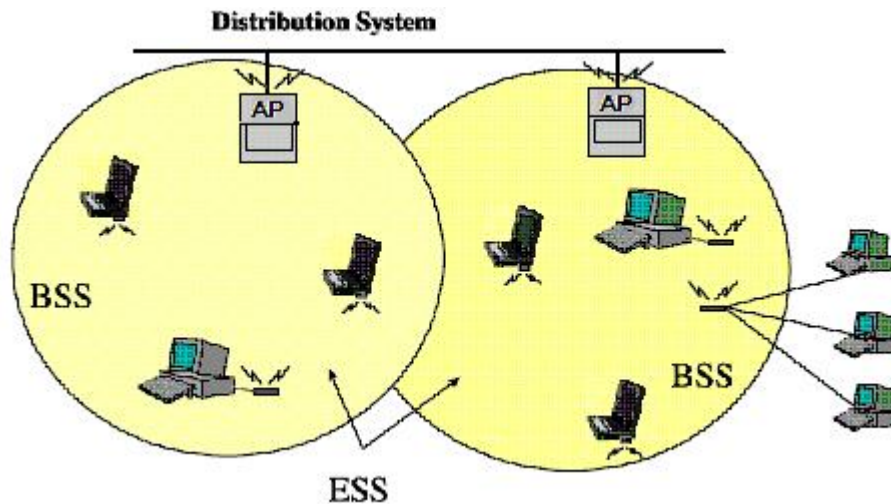


Figure 2 802.11 Wireless LAN

not use this functionality of fixed access points, but participating nodes are required to communicate with each other and build relationships so to carry out WLAN functionality.

To gain access to a WLAN, the user equipment must first acquire synchronization information concerning that wireless network. This is accomplished by the user equipment either passively scanning its nearest access point to wait to receive a Beacon Frame or actively probing access points by sending a Probe Request. Beacon frames contain the value of an AP's clock at the time of transmission and are used by a mobile client to learn an AP's transmission schedule. Once the user equipment has found an available AP, IP logical addressing must be extended to the mobile client.

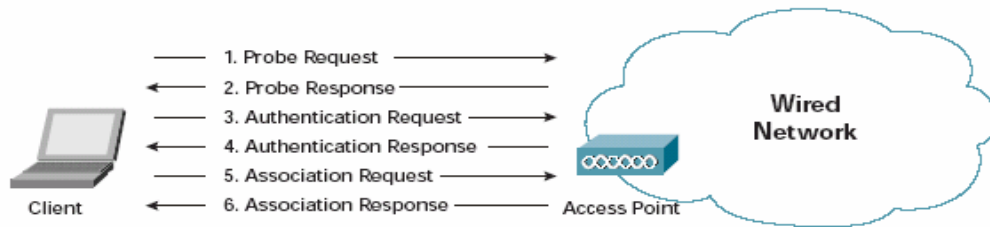


Figure 3 802.11 Client Authentication Process

A DHCPDISCOVER broadcast message is sent by the mobile client containing its MAC hardware address to find a DHCP server on the WLAN. Once a request for an IP address is received, the DHCP server responds with a DHCPOFFER message containing an available address and configuration parameters. The mobile station accepts the temporary address by sending a DHCPREQUEST message to the server which acknowledges to the client with a DHCPACK message. The mobile station's assigned IP address and MAC address are forwarded to the WLAN authentication server in order to initiate authentication. Authentication and association must be completed before the user is allowed to transmit or receive any data frames within the WLAN. Security is implemented in WLANs so to prevent unauthorized access to private network resources and to protect the privacy and integrity of transmitted user data.

3G-WLAN Integrated Architecture

Fundamentally different approaches have been defined to integrate 3G and 802.11 WLAN networks. The *tight coupling* approach defines development of enhanced hardware that integrates processing of 3G physical layer protocols in 802.11 networks [3]. This new hardware accessing the GPRS network will manage subscriber mobility and user sessions for WLAN users. The *Loose coupling* approach, conversely, allows for access to the 3G core network from within WLANs without fully implementing 3G protocol processing in existing 802.11 network equipment [9]. New protocols for the public IP backbone have been designed to implement 3G user management for users of potential WLAN areas. The accurate implementation of 3G-WLAN internetworking providing secure access to 3G services from WLANs is essential to the successful convergence of these network technologies.

Integrating 3G and WLAN networks requires dual mode user equipment possessing both wireless transceivers, 3G and IEEE 802.11. Dual mode user equipment is

currently available to subscribers and will be the standard for the future. An example of a *tight coupling* internetworking approach requires an enhancement to 3G core network hardware so that SGSN nodes can process 802.3 MAC frames transmitted from the distribution system of a WLAN. A GRPS Internetworking Function, GIF, defines the capability to process both 802.3 and 3G MAC layer protocols making the SGSN unaware of the type of network from which the 3G user's packets originated [3]. A WLAN adaptation function, or WAF, would provide internetworking at the SGSN by translating 802.3 MAC frames into GPRS MAC frames [3]. Additionally, user equipment would be enhanced with the WAF to encapsulate 802.11 MAC into 3G Logical Link Control PDUs. The required 3G and IEEE 802 protocols that these new hardware components will process are diagrammed and described below.

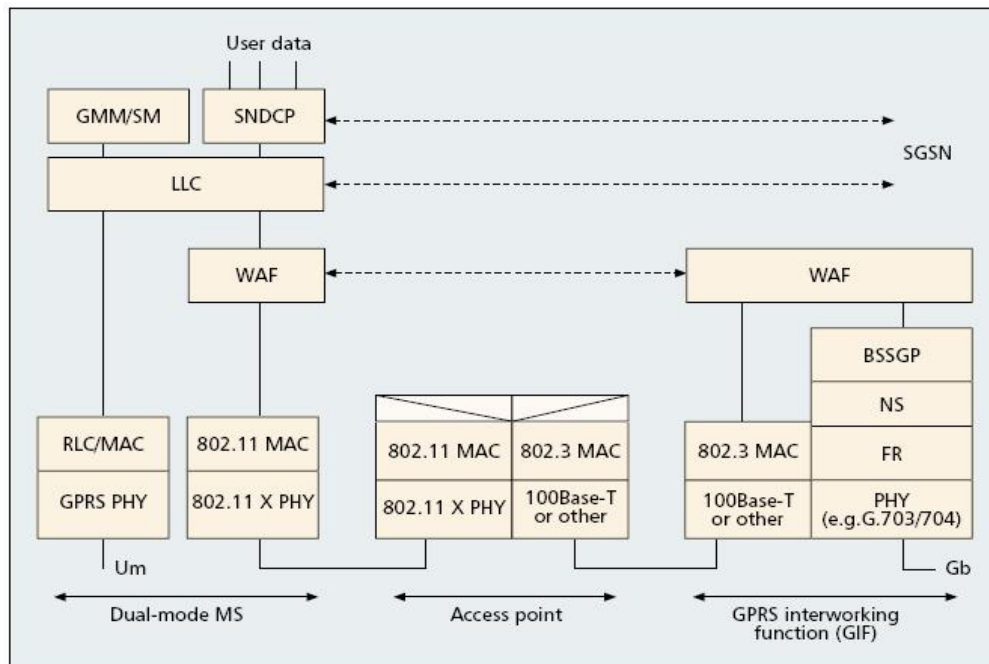


Figure 4 Protocol Architecture for Tight Coupling

- PHY** G.703/704 physical communication in the core network
- RLC** Radio Link Control in user cellular equipment
- FR** Full Rate voice encoder for speech transmission in the core network
- NS** Network Service indicating congestion in the core network
- BSSGP** Base Station Subsystem GPRS Protocol transports MAC layer functional information to the core network from a base station
- SNDCP** Sub-network Dependent Convergence protocol performs compression, multiplexing and segmentation

In this *tight coupling* internetworking example, both 3G network and user equipment must be enhanced to encapsulate 3G and 802.11 physical, PHY, and media access control, MAC, protocols. The benefits of this *tightly coupled* internetworking approach are that full 3G functionality is accessible from a visited WLAN network. 3G users are authenticated and initiate sessions by utilizing currently defined processes and protocols implemented within the 3G standards. This example demonstrates how quality and integrity of current 3G mobility and user management procedures are not disrupted by a *tightly coupled* implementation. The following diagram depicts a tightly coupled

network in which a WLAN interfaces directly to the 3G core network via newly defined inter-networking functions and hardware [3].

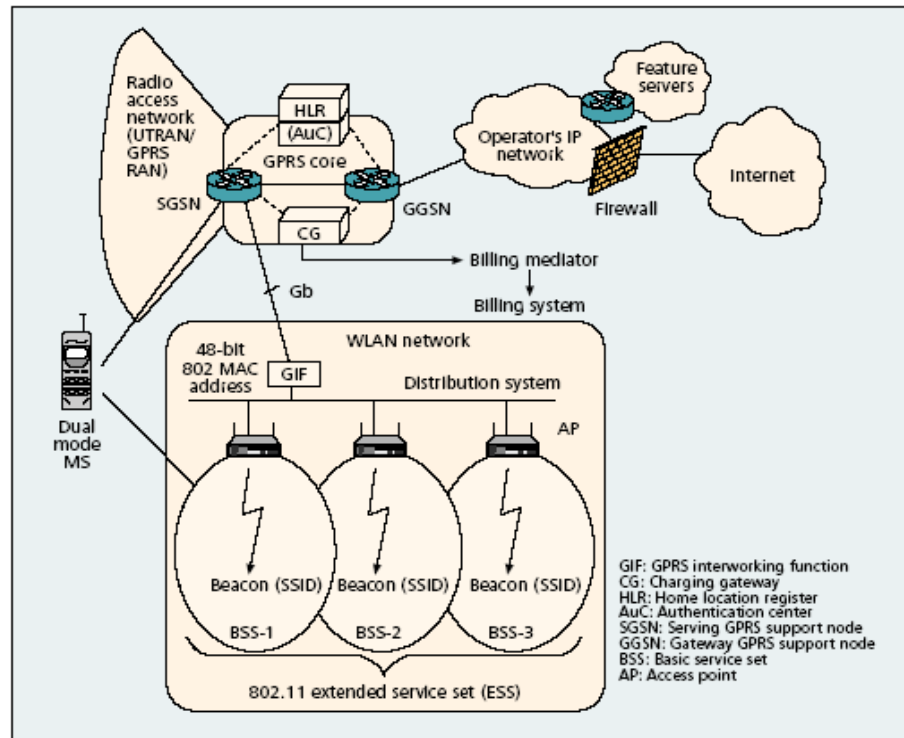


Figure 5 3G-WLAN Integration with Tight Coupling

However, the drawback of this integration approach is the cost associated with designing and manufacturing new infrastructure and user hardware. All Serving GPRS Support Nodes, SGSN, would require integration of new firmware to provide access to the 3G core network from 802.3 networks. Additionally, current user equipment would need to be enhanced with the functionality to communicate low level 3G protocols over WLANs.

A *loose coupling* approach has been adopted by researchers and industry leaders to mitigate these potential obstacles associated with deploying new dually enabled 3G and 802.11 hardware. Potential 3G-WLAN integration can be implemented with the approach that a WLAN is treated as a publicly visited network that stands complementary to the 3G core network. Authentication and session management is performed for WLAN users requesting 3G access via new protocols transported over the IP backbone to the 3G core network without accessing the 3G radio transport network. New protocols are required to deploy a *loose coupled* integrated network, but a significant benefit of this internetworking option is that no low level protocol processing needs to be integrated into existing network or user hardware. Figure 6 highlights a WLAN network's access to the 3G core network through the IP backbone [3]. This *loose coupling* integration allows faster deployment of hybrid 3G-WLAN access networks and deserves careful study as to how to effectively implement 3G user policies and procedures for WLAN users. User authentication, session key agreement, and billing procedures will be issued over the IP backbone versus traditional 3G access networks. It is critical that the design of these IP protocols preserve the quality of existing 3G protocols and that the potential security risks of 3G-WLAN integration are identified and resolved.

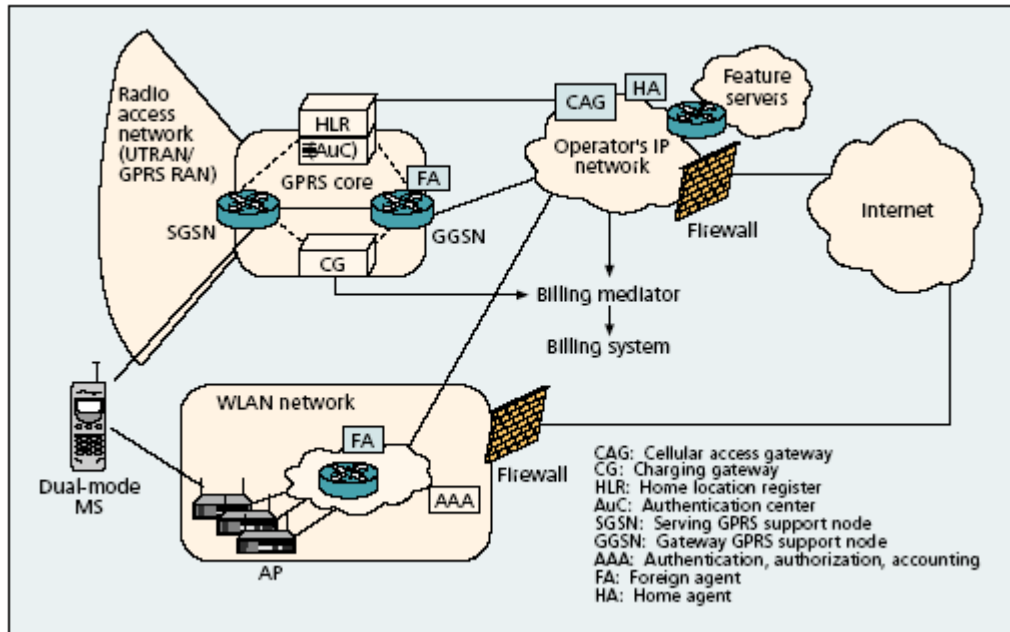


Figure 6 3G-WLAN Integration with Loose Coupling

3G Security Architecture

Current cellular network security procedures have been redesigned for future 3rd generation networks. Existing procedures implement authentication, key agreement and data encryption between the user equipment and cellular network. The 3G security protocol provides enhanced authentication and has been designed to answer weaknesses in the existing 2G security protocol. The 3G security architecture defines mutual authentication between the user and cellular network, new encryption algorithms and better freshness of user cipher and integrity keys. Security algorithms have further been enhanced by the use of longer keys to create stronger user authentication and data encryption.

In 3rd generation authentication procedures, each subscriber is identified by his/her unique International Mobile Subscriber Identity, IMSI, which is stored in the USIM module within the user's equipment and at the 3G HLR database. Each subscriber is assigned a unique 128-bit secret key, K_i , which is stored in the user's SIM and 3G authentication center, AuC. All authentication algorithms are performed internally in the user's SIM and at the 3G AuC using the 128-bit subscriber key K_i . 3G encryption algorithms used to create a user's authentication challenge, integrity, confidentiality keys and network authentication code are significantly strengthened by the use of the Rijndael AES block cipher algorithm. The AES block cipher can be customized by 3G operators who are allowed to set 10 intermediate constants $c1-c5$, $r1-r$ used as variables by the algorithm plus set a 128-bit operator specific variant configuration field, OP [5]. With an order of 10^{21} times more AES 128-bit keys than the 56-bit keys of 2G DES encryption, AES key recovery using current key-exhausting algorithms is considered unachievable.

3G user authentication occurs when a user's equipment is initially powered on and subsequently performed as user moves throughout the 3G access network or

performs a service request. As a cellular user travels through his/her provider's network, low level connections are maintained between the user and 3G core network. A user's VLR/SGSN will communicate with the cellular core network updating the user's current location and session information at the core network. The area serviced by a VLR is designated as a Location Area, LA, or a Routing Area, RA. As a user's LA/RA changes, he will be prompted for re-authentication by his new VLR or SGSN.

However, inter-SGSN RA updates do not necessarily prompt user re-authentication as defined by 3G policies [14]. A user's current location is stored by the 3G HLR in the form of a Location Area Identifier, LAI, which is used to uniquely identify a LA. A LAI is comprised of a 3 digit Mobile Country Code, MCC, 2-3 digit Mobile Network Code and 2 byte Location Area Code [14]. Furthermore, in order for a user's MSC/SGSN to be able to route calls or packets to a user located within an LAI, a 2 byte Cell Identity, CI, is appended to a user's LAI to distinguish what is the user's current cell.

When a user's current VLR/SGSN changes, a mobility management location update request is initiated by the new VLR/SGSN to the 3G core network [14]. User mobility management is executed via the MM protocol to exchange data to the cellular core network notifying a mobile user's present location and subscription information.

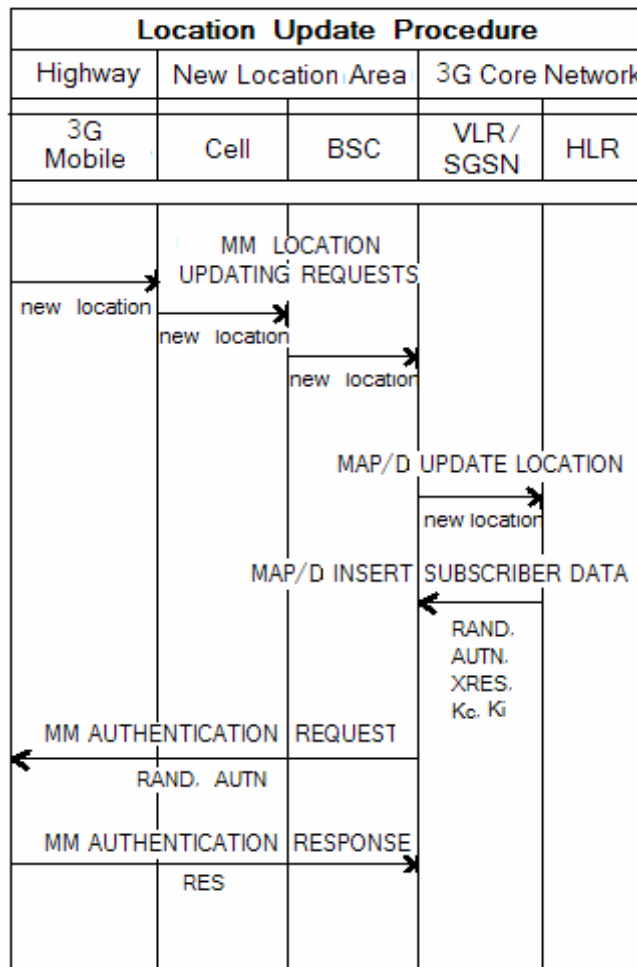


Figure 7 3G Location Update Procedure

The user's current location is carried from the core network to a central cellular database or Home Location Register, HLR, by the MAP/D protocol, upon entry to a new location area service by a different VLR/SGSN. The HLR database located within cellular headquarters stores private user management data, including user identity and secret subscriber key. Entry into a new location area serviced by a different VLR/SGSN prompts user re-authentication to the 3G network. Once a user's location has been updated to the HLR, the MAP/D carries authentication credentials back to the VLR/SGSN from an Authentication Center, AuC, to re-authenticate the user. The following sequence diagram illustrates the MM and MAP/D protocol exchanges as a user travels into a new location area.

To generate user authentication credentials, the 3G HLR will retrieve the respective user's secret key K_i from the AuC. The HLR generates a 128-bit random number, RAND, and uses the random number as an input value to obtain the user's expected authentication response, SRES, integrity and confidentiality keys, IK, CK and a network authentication code, AUTN. The HLR will send a set of authentication quintets composed of {RAND, SRES, IK, CK, AUTN} for the user to the requesting VLR/SGSN [14]. The VLR will choose an authentication quintet for the user and forward the authentication challenge, RAND, and network authentication code, AUTN to the user.

Executing the same authentication algorithms within his/her SIM, utilizing his/her secret 128-bit key, K_i , and received RAND challenge, the user will first authenticate the 3G network. The network authentication code, AUTN, is constructed using the user's sequence value, SQN, which is kept current within the user's SIM and 3G HLR database. The user's sequence number is encapsulated by the user's anonymity key AK, and

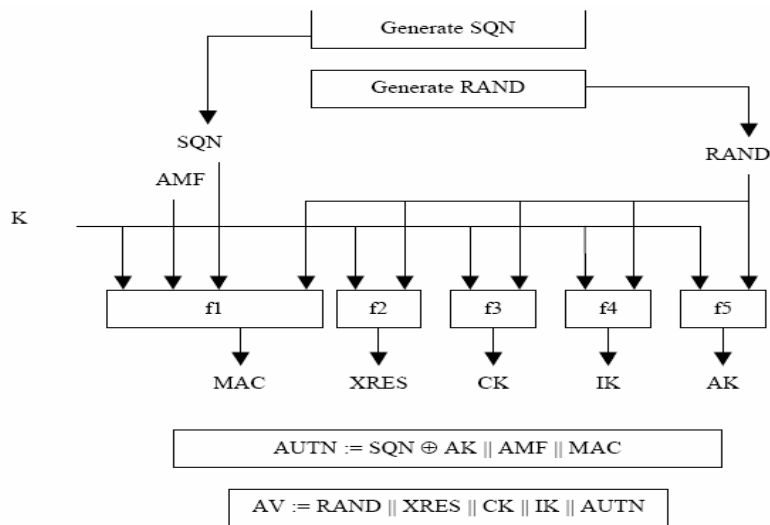


Figure 8 3G Security Algorithms

appended with an authentication management field, AMF, and message authentication code, MAC to create the AUTN. Upon receipt of a network authentication code, the user will calculate the expected MAC for the message, XMAC, based on his SQN and K_i and the received AMF and RAND. If the calculated XMAC equals the received MAC and the received SQN is number within an accepted range of the user's stored SQN, the authentication challenge is accepted by the user equipment. Otherwise the user will send

an *authentication reject* message back to the VLR/SGSN and abandon the procedure [14]. The user can also send a *resynchronization request* message to the VLR/SGSN prompting an exchange between user equipment and HLR to acquire user SQN synchronization.

At successful verification of the 3G network, the user SIM will generate and send an authentication response, RES, back to the VLR/SGSN. Upon verification of the equivalence of the RES received from the user and the SRES present in the chosen HLR authentication quintet, the VLR/SGSN will notify the user of authentication success [14]. The VLR/SGSN then forwards the cipher and integrity keys, CK and IK, from the chosen HLR authentication quintet to the user. Upon successful authentication, a user will regain secure access to the cellular network utilizing session keys assigned by the AuC to protect user confidentiality and data integrity. This enhanced authentication process is diagrammed in Figure 9.

The 3G security architecture builds mutual authentication between the user and 3G network, and implements strict user data confidentiality and integrity. However, user privacy must be maintained as he/she interacts with the 3G network. Additional security is required to protect the real identity of users and to disallow tracking of users' mobility. A temporary mobile subscriber identity, TMSI, assigned by a user's VLR/SGSN, is used over the cellular access network to protect the real identity and privacy of mobile users [14]. Primarily, any association between a user's location and subscription management data and his/her true identity, IMSI, is disallowed. Use of temporary identities, TMSI, prevents tracking of a user's activity or movement by

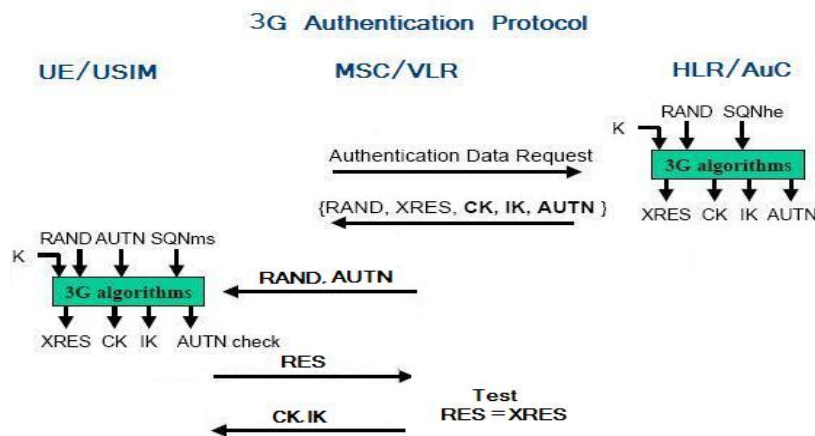


Figure 9 3G User Authentication Process

an eavesdropping party. A user's temporary identity is assigned at re-authentication or entry into a new location area and is valid for the time the user is active within that location area. A packet TMSI, P-TMSI, is the equivalent temporary id assigned to a user connected to the packet core network via an SGSN. Once a user has re-authenticated to the cellular network and ciphering becomes enabled, a new TMSI is allocated and sent to the user by his VLR/SGSN. Sent in encrypted format, the new TMSI cannot be associated with the subscriber. The core cellular network identifies a user by his/her

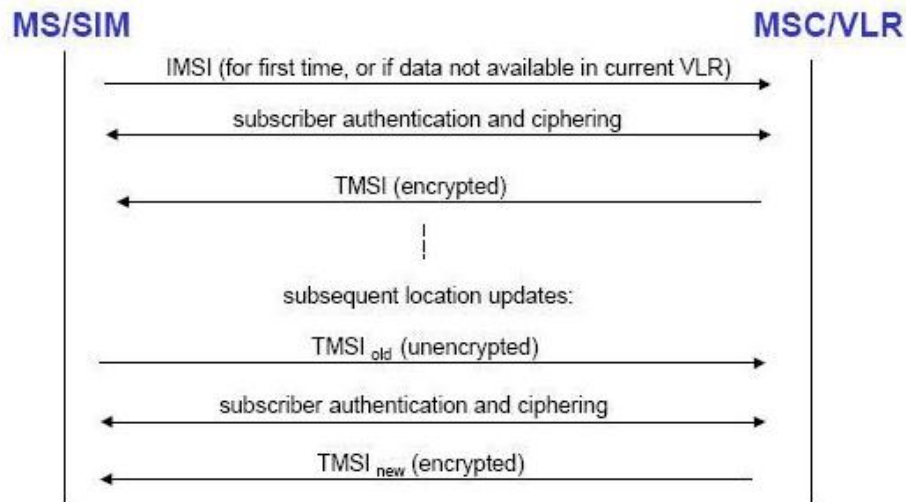


Figure 10 3G Temporary User Identity Assignment

TMSI for all following subscription management procedures. The allocation of temporary identities is diagramed above.

802.11 WLAN Security

Security over 802.11 wireless networks poses more risks than traditional wired networks since wide physical areas are made available to many potential users. Initial 802.11 WLAN security implemented entity authentication and data encryption defined by the Wired Equivalent Privacy standard, WEP. Entity authentication included *open system* and *shared key* authentication. A WLAN access point would grant access to anyone that requested it in open system authentication, while shared key authentication depended on a secret key being shared between the requestor and authenticator. A secret key would be used to encrypt the authentication challenge received from an access point by a user requesting access to a WLAN. If the access point could successfully decrypt the correct challenge using the user's secret key, access was granted. Data integrity and privacy implemented in WLANs was initially implemented using the 40-bit stream cipher RC4 algorithm. The 802.11 standard, WEP, supported static predefined shared keys for data encryption transmitted between access points and user equipment. Initial WLAN security was easily breached and the vulnerabilities presented prompted the redesign of WLAN security algorithms. For instance, if an open system authentication was filtered by an access list of legitimate user equipment MAC addresses, access could be easily acquired by an eavesdropper that captured MAC addresses sent in clear text over the WLAN [15]. This vulnerability also existed for WLANs that limited access to users possessing knowledge of the WLAN server set ID, SSID, used to uniquely identify WLAN networks. With SSIDs broadcasted in clear text by serving access points, maintaining controlled access to a WLAN became threatened. Additionally, shared key authentication algorithms were vulnerable to man-in-the-middle attacks in which a clear authentication response and the corresponding cipher text could be captured by an eavesdropper [15]. With the possession of both the clear and cipher text pair, an attacker could successfully derive a user's shared key. Initial WLAN security also required difficult configuration since authentication keys could be integrated into user 802.11 WLAN adapters. The loss

or theft of a user's adapter created vulnerability for a WLAN and significant management challenges to the operator.

The 802.11i standard was introduced to enhance existing WLAN security. The goal of the 802.11i standard is to define *robust security network associations* so that all relationships between parties are built on strong authentication and association, or *RSNA* [8]. The 802.11X framework is integrated into 802.11i to deliver authentication services and key management. The new framework answers the initial weakness of WLAN authentication, implements stronger encryption algorithms and provides dynamic session key management incorporating a four-way handshake. 802.11X defines the components of a WLAN as *supplicants*, *authenticators* or *authentication servers* by the 802.11i standard. A supplicant is the mobile node requesting WLAN access and the authenticator represents the network access server, which in WLANs are access points. The authentication server is a new component implemented into 802.11 security and is either a RADIUS or DIAMETER access server. The 802.11X framework is *port-based* in which a port is defined between the supplicant and authenticator. All traffic is blocked for an existing port, except 802.11X messages, until a supplicant is authenticated. Several mutual authentication schemes are available for WLAN authentication, i.e. MD5, TLS, EAP-SIM, with the Extensible Authentication Protocol, EAP, employed for transporting authentication messages between the supplicant and authentication server. Improving upon the weak *entity authentication* and static *shared key* authentication defined by 802.11, the 802.11X framework authenticates the WLAN user and allows the user to mutually authenticate the WLAN network eliminating man-in-the-middle attacks from false access points.

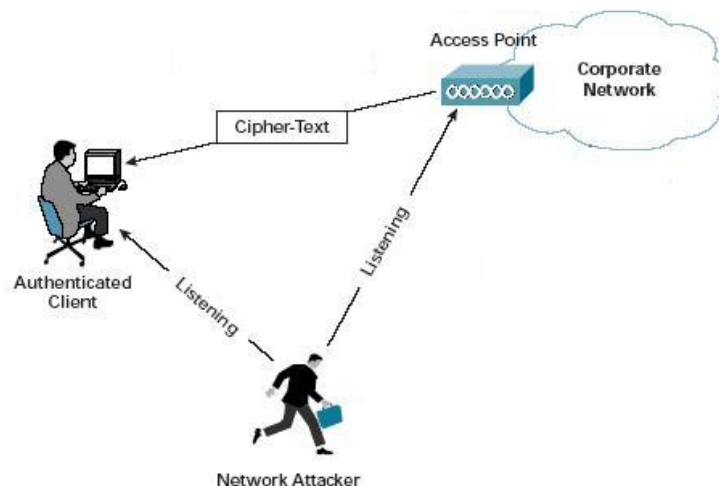


Figure 11 WLAN Man In the Middle Attack

RSN information elements carry security information indicating authentication and cipher algorithms the parties will use for WLAN communication. Mobile nodes and WLAN access points learn of the security capabilities of their peers via RSN IE messages and negotiate as to which security suite to use. The 802.11 weakness of an attacker deriving WEP RC4 initialization values has been resolved by the introduction of a 128-bit temporal key algorithm, TKIP. The temporal key, TK, is a shared secret key between the user and authentication server that is built from a client's MAC address to ensure key uniqueness between mobile users. The communicating parties must ensure that no

initialization vector, IV, is used more than once for a current TK. The shared TK is updated before the full 48-bit IV space is exhausted to ensure robust IV use. TKIP also implements packet sequence counters such that out-of-order packets are dropped to prevent replay attacks. Since TKIP employs the older RC4 stream cipher, the 802.11i standard includes a second encryption option to utilize new advanced encryption standards. 802.11i defines the CCMP algorithm using the AES CCM mode with a 128-bit key and 128-bit block size of operation.[8] CCM employs AES counter-mode, CTR, to encrypt packet payload and cipher-block chaining, CBC-MAC, to build message authentication codes to provide message integrity and confidentiality. A fresh TK is required for each session and packet numbers, PN, are implemented to prevent replay attacks.

3G-WLAN Security Architecture

Implementing 3G authentication over the IP backbone is critical to rapidly and inexpensively merge 3G and WLAN networks. Basic functions for subscriber management performed by 3G network hardware must be accessible to users within WLANs desiring access to 3G services. User authentication must be implemented successfully using the IP backbone to allow 3G network access from popular, visited WLANs. Proxy functions integrated into existing servers have been identified to facilitate 3G subscriber management and serve as the critical connection between WLAN and 3G networks.

Placement of 3G Authentication, Authorization and Accounting services within *loosely coupled* 3G-WLAN networks has been defined to implement the integrity of 3G user security over WLANs. These 3G AAA servers will communicate with counterpart AAA proxies integrated within visited WLANs. AAA servers will access the core network HLR so to initiate 3G user authentication for WLAN users. Requests for authentication will be transported between WLAN AAA proxies and 3G AAA servers via an enhanced IP transport protocol. The transport protocol EAP, or Extensible Authentication Protocol, defined for 802.11 WLANs, has been extended to service 3G

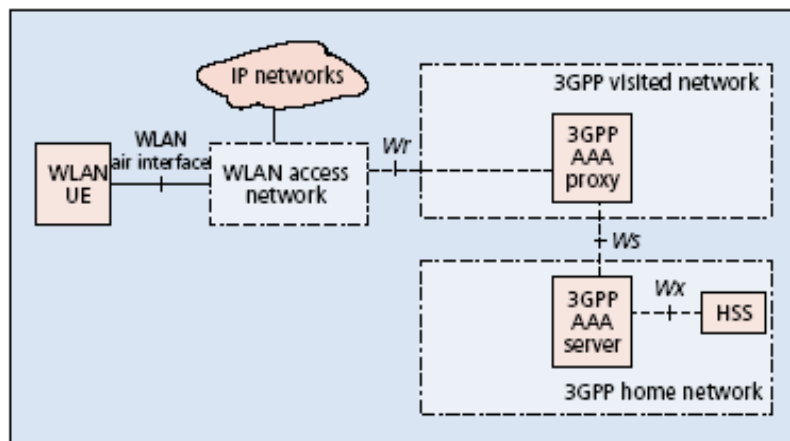


Figure 12 3GPP-WLAN Internetworking Architecture

SIM-based authentication exchanges initiated from WLANs [8]. The EAP extension defined for transporting the 3G Authentication and Key Agreement procedure to and

from a WLAN is designated EAP-AKA. The sequence of events occurring during the EAP-AKA process is diagrammed in Figure 13.

Upon entry to a WLAN, a 3G-WLAN AAA proxy will prompt the user for his 3G user identity. A WLAN user will identify himself to the AAA proxy via a Network Access Identifier, NAI, composed of a username and realm or network name delimited by the @ sign. Aliases are allowed for the username portion of the NAI to protect 3G user privacy while he/se visits a WLAN [1]. The EAP authentication request is then forwarded to a AAA server within the 3G home network. The 3G HSS is notified of the user's authentication request and prompts the HLR to generate 3G authentication vectors to be transported back to the 3G AAA server. The HSS, Home Subscriber Server, has been designed for 3G-WLAN integration and provides connectivity to a subset of services performed by the 3G HLR [5]. Upon receipt of a WLAN user's authentication vector, the 3G AAA server performs the responsibilities traditionally delegated to a 3G VLR/SGSN by sending an authentication challenge, RAND, and network authentication code, AUTN, to the WLAN user. Upon the user's successful authentication of the 3G network using the AUTN code and sending his/her correct challenge response to the AAA server, the user will be notified of his/her successful authentication and allowed access to 3G services. 3G authentication algorithms, present only at the 3G core and user equipment USIM, that apply the user's unique secure key K_i to create 128-bit authentication credentials are used by the EAP-AKA protocol to authenticate a 3G user from within a WLAN [5].

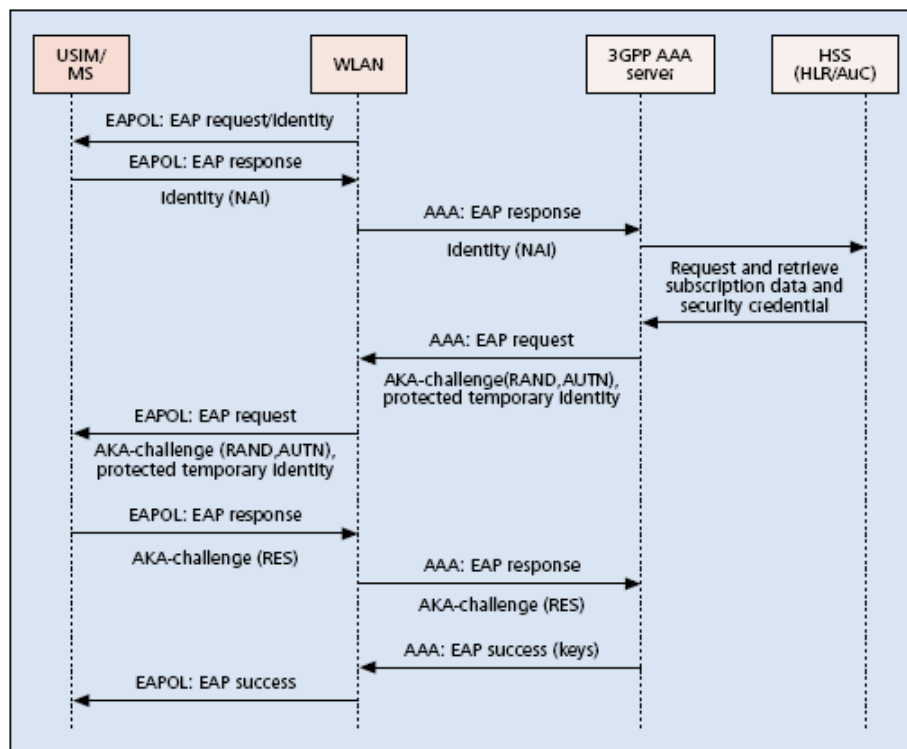


Figure 13 AKA Procedure between 3GPP and WLAN Networks

Successful implementation of the EAP-AKA protocol relies on secure transport of EAP packets between a WLAN AAA proxy and 3G AAA sever. The EAP protocol,

initially designed to implement 802.11 WLAN user authentication, details a transport mechanism to transfer user authentication challenges and responses between a WLAN and a remote authentication server. A secure peer relationship is created between WLAN AAA proxies and 3G AAA servers so to successfully transport EAP authentication payloads over the IP backbone using the DIAMETER transport application [11, 12]. 3G user authentication challenges and responses are transferred from a 3G AAA server to a WLAN via the Diameter-EAP-Request and Answer messages, DER and DEA. These messages include components to initiate a unique session between the WLAN AAA proxy and 3G AAA server. The participating WLAN AAA proxy is identified by an Origin-Host and Origin-Realm name and the targeted 3G AAA server is designated by Destination-Host and Destination-Realm within the Diameter messages.

```

<Diameter-EAP-Request> ::= < Diameter Header>
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }
    { EAP-Payload }
  
```

The EAP-Payload encapsulates the EAP packets when transferred between a WLAN and 3G AAA proxy and server. To protect 3G user authentication, DIAMETER exchanges are encrypted by implementing either IP security, IPSec, or IP transport layer security, TLS. The relationship of DIAMETER clients and servers within a 3G-WLAN integrated network is diagrammed below.

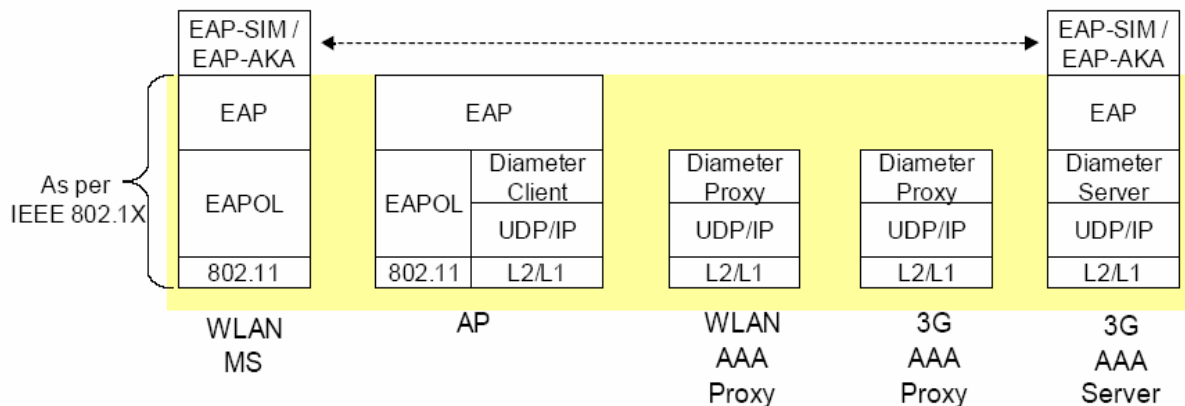


Figure 14 DIAMETER Protocol between WLAN and 3GPP Network

The DIAMETER protocol ensures that EAP-AKA authentication requests are initiated from an acceptable peer. The vulnerability that EAP-AKA requests are forged from a non-DIAMETER capable node is eliminated by the required relationship between 3G-WLAN AAA servers and proxies. To ensure EAP messages are not manipulated when transferred between 3GPP and WLAN networks, the Cryptographic Message Syntax (CMS) is implemented by DIAMETER to detect fraudulent proxies that may modify data within messages [13].

Once authenticated from within a WLAN, services provided over the 3G private network will be accessible to subscribers. Example services include Multimedia Messaging Service, MMS, and 3GPP IP Multimedia Subsystems, IMS. Tunneling will be additionally employed between the 3G private IP network and WLANs to deliver user packets securely. Routing contingencies are also available so that if a WLAN access network can not route packets to the 3G home network, user equipment can learn and choose from WLANs capable of routing to his/her 3G provider [5]. Charging information will be collected for a WLAN user as data packets are routed through the 3G owner's private network. This 3G-WLAN integrated infrastructure creates opportunities for sharing rich integrated data and voice services to mobile users. The maturity of 3G-WLAN integration creates significant value for future networks.

Risk Analysis of 3GPP-WLAN Security

Potential vulnerabilities presented by 3G-WLAN network integration in a *loosely coupled* architecture must be defined. The merging of 3G and WLAN networks will prompt a higher volume of delivered rich data services and access to sensitive user data over wireless networks. Interactive video and conferencing will increase and the access to sensitive corporate data and files will be available over 3G-WLAN networks. With richer services and sensitive, valuable user and business data accessible from more wireless access networks, the risk of dishonest attempts for access will increase. The different types of threats presented to the 3G home network providing access to services from WLANs include:

- illegal access to 3G services
- prevention of access to 3G services
- unauthorized access to 3G user data

The purpose of this paper is to define algorithms that minimize the threat of illegal access to 3G networks from WLANs. The transport of EAP-AKA authentication requests over the IP network introduces a new threat to 3G networks. The IP backbone is a partial mesh network of which the origin or validity of an EAP-AKA authentication request may not be readily verified by the 3G core network. An attacker may impersonate a valid user by requesting EAP-AKA authentication from a WLAN that results in the victim being charged with the attacker's illegal usage of services. An attacker can successfully impersonate a valid user if he possesses knowledge of a user's IMSI and subscriber key, K_i , and creates falsified EAP-AKA authentication messages. This form of illegal access is particularly dangerous to 3G networks since it can be performed remotely over the Internet with the attacker not physically present in a WLAN. The prior "open" environment of WLAN networks, in which messages from access points are sent in clear text to users, also poses a threat to 3G services access in which an attacker can steal a user's MAC/IP address combination and access a user's wireless session. With the current 3G-WLAN security architecture, the 3G home network gains limited knowledge or warning of illegitimate activities or behavior of users within the WLAN.

The potential threat to 3G networks that provide service access to WLANs is significantly impacted from the mixed, different ownership of the integrated wireless networks. Authentication for traditional 3G network access originating, from 3G owned cells, is initiated and executed by secure 3G VLR/SGSN nodes. Authentication vectors

travel through strict paths within the 3G hierarchical infrastructure to the user's active location area where user authentication is performed. The home network can trust that invalid 3G authentication requests have not been interjected into the cellular radio access network. Unlike security initiated from a 3G cell, however, WLAN access networks may not be an extension of 3G access networks and may be owned by different operators. Furthermore, the 3G operator may possess no knowledge or relationship with potential WLAN owners. It is essential that the 3G home network gain knowledge of the integrity of WLAN partners so to prevent abusive access to 3G service access. The 3G network may be unaware if an EAP-AKA request is interjected illegally via a dishonest user connecting to a WLAN AAA proxy. Additionally, the 3G home network is vulnerable if the WLAN operator initiates invalid authentication requests on behalf of a dishonest attacker. This paper presents security algorithms that enable the 3G home network to gain robust assessments of WLAN networks and their EAP-AKA security performance. Algorithms are proposed that enable the 3G home network to protect itself from illegal authentications originating from IP serving networks or WLANs. The 3G home network can exercise these new security mechanisms to verify the authenticity of EAP-AKA requests and prevent unauthorized access.

Enhanced EAP-AKA Security Protocol

Authentication Control in EAP-AKA Protocol

The EAP-AKA process must be enhanced so to eliminate unauthorized access to 3G networks and services from WLANs. It is beneficial to control 3G authentication, initiated from a WLAN, in such a way that it can only be successfully completed by an intended recipient or within the intended WLAN access network. This can be accomplished by encrypting EAP-AKA authentication vectors such that successful decryption is dependent on knowledge of user specific data, additional to the user's unique key K_i , or user location. For instance, the following 3G user state information can be used to encrypt a user's EAP-AKA authentication challenge so that it can only be deciphered by the intended user. Encryption can be accomplished by XORing the user's authentication challenge with the following state data prior to forwarding the challenge to the user's WLAN:

- user's current LAI or CGI
- user's current TMSI
- user's current SQN
- user's equipment serial number

Upon receipt of the XORed authentication challenge, a user must extract the original challenge before proceeding with SIM-based authentication processing. These bits of data are very powerful in limiting 3G authentication to a targeted subscriber that requests access to services over an IP network. The risk of a 3G user's identity being forged via a dishonest EAP-AKA authentication request can be mitigated using this approach. However, the 3G user state data listed does not provide the strongest protection for controlling 3G-WLAN authentication. For instance, a LAI/CGI assignment is static data that can be obtained by an intelligent attacker who determines the location area a vulnerable WLAN resides in. A user's authentication sequence number, SQN, is not unique between users, requires synchronization between the user equipment and 3G core network and is only a 48-bit value which creates the opportunity for attackers to derive the key using a brute-force method. Encryption using a user equipment serial number requires an added protocol exchange at the 3G home network between the HLR and EIR which is currently implemented on a limited basis. Furthermore, the 3G core network is not aware of user's current TMSI since it is assigned and stored at the user's current VLR/SGSN.

Spatial Control in EAP-AKA Protocol

A feasible option for enhancing 3G-WLAN security is to limit successful authentication to a targeted area in which a user resides such that the authentication challenge can be responded to from that area only. Controlling *where* successful authentication can be executed provides a more robust approach to protecting 3G service access initiated from WLANs. EAP-AKA authentication credentials can be encrypted so that successful application requires physical occupancy within a targeted specific area. For instance, a 128-bit Area Descriptor, AD, defining an area within a WLAN can be used to encrypt a user's authentication challenge. The challenge can only be decrypted

and used from within the limited target area defined by the AD. 3G user authentication architecture can be readily enhanced to implement spatial control of 3G-WLAN user authentication. Both the user equipment and 3G home network hold the knowledge required to build the user's current area descriptor which can be used to encrypt the user's authentication challenge. With a user's 3G home network determining an area descriptor AD_{HN} for the user, the user's authentication challenge $RAND$ can then be encrypted using some function $F()$ to produce $RAND_{AD}$ [6].

$$AD_{HN} \wedge RAND = RAND_{AD}. \quad (1)$$

Upon receipt of his authentication challenge, the user can decrypt $RAND_{AD}$ using the same function $F()$ and his own defined area descriptor, AD_{UE} , as a key.

$$AD_{UE} \wedge RAND_{AD} = RAND. \quad (2)$$

3G SIM authentication algorithms can then be executed using the user's subscriber key K_i and original $RAND$ to deliver the authentication response, RES , to the 3G AAA server. Encrypting a user's authentication challenge with spatially related data successfully limits 3G user authentication to within the specified WLAN area only. This enhanced EAP-AKA procedure builds stronger 3G user authentication initiated from visited WLANs and limits the vulnerability of unauthorized access to 3G network services from WLANs.

Several options exist for defining a 3G-WLAN user's Area Descriptor, AD, or location to be used in an enhanced EAP-AKA algorithm. Simple geometric shapes such as ellipsoids or polygons, with a defined area of uncertainty, can be used to delimit a user's login area. Real geo-coordinate data, or latitude and longitude, can designate the points necessary to create a user's area descriptor, such as the central point for an ellipsoid or end points for a polygon. A relative coordinate system defined by a WLAN operator can be used to provide relative geo-coordinate data to define a user's area descriptor or precise user location can be obtained via location algorithms implemented within WLANs in which beacons advertising the absolute coordinates of access points are used by receiving mobile equipment to calculate a current position. Alternatively, the WLAN operator can define regions or sub-areas within the WLAN coverage area and notify the user his/her assigned area. A 3G network is not capable of determining a user's location coordinates at the precision required to bind a user authentication to a small WLAN network. Thus, data designating a user's location can be forwarded to the 3G home network at the event of a user's EAP-AKA authentication request from the WLAN AAA proxy. The 3G authentication challenge can then be encrypted using the spatially dependent data defining the user's location.

The primary obstacle to implementing spatial control for user authentication in 3G-WLAN networks is that user privacy must be retained. Users of 3G services are not required to reveal their location to their network provider unlike mobile participants in private networks used for industry or government. A 3G user's precise location coordinates can be obtained by the core network in the event of emergency E911 service request only. Otherwise, the home network is incapable of identifying a user's location other than his/her current location area, LA/RA, which can range from over 50 to 100

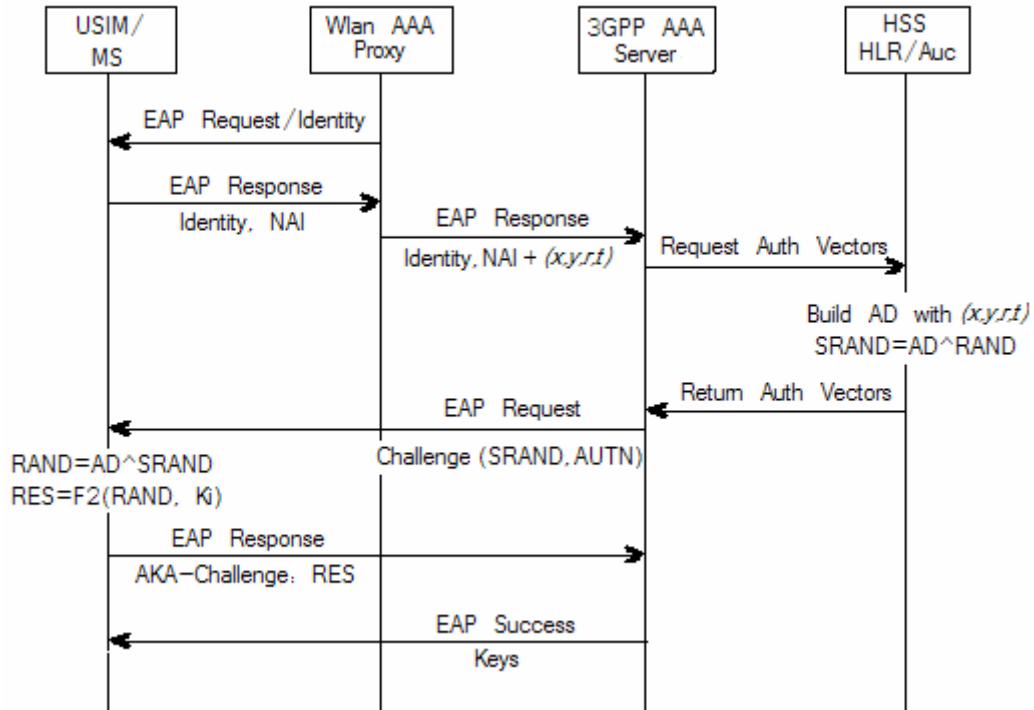


Figure 15 EAP-AKA Protocol with Spatial Control

square miles. A 3G subscriber possesses control of his location privacy and 3G security algorithms are designed to protect that privacy. Enforcing spatial authentication control for 3G-WLAN integrated networks must implement these specific restrictions to protect user privacy.

Thus, the most feasible implementation of a spatially dependent EAP-AKA protocol requires that the 3G home network depend on user’s spatial coordinates sent from serving WLAN access networks. The 3G network must trust the spatial data provided for a user by the serving WLAN network when this enhanced EAP-AKA algorithm is used. The spatial EAP-AKA algorithm becomes more reliable when a trust relationship is defined and maintained between the 3G home network, *HN*, and serving WLAN network, *SN*.

Risks of Spatial Control in EAP-AKA Protocol

Spatial control for 3G EAP-AKA user authentication is intended to mitigate abuse of illegal 3G network access from WLANs by limiting authorization to within the WLAN in which the user is present. Remote subscriber impersonation from anywhere on the Internet can be eliminated as a user is required to associate with a WLAN network before requesting 3G network access. The user’s authentication challenge is encrypted with his specific WLAN area descriptor requiring his physical presence within the WLAN. Spatial control for user authentication can be very powerful when unique sub-areas are defined for each WLAN user. Gaining access to a user’s authentication or other sensitive data becomes more difficult as the spatial key used for encryption becomes more complex and unique. The efficacy of spatially controlled user authentication increases as unique sub-areas define users’ area descriptors. The 3G home network, however, has no means of

measuring the validity of geo-coordinates sent with a EAP-AKA request. Established subscriber privacy policies would be breached if the 3G network verified the user's location to the resolution required for the small visited WLAN area. The potential exists in spatially enhanced EAP-AKA, for an attacker to use false geo-spatial coordinates and still be authenticated to the 3G network. An attacker can mimic the functionality of a WLAN AAA proxy by sending the required EAP-AKA request to the 3G network with augmented spatial data. Thus, an ineffective step is added to the EAP-AKA protocol that does not protect 3G user authentication and can be readily abused by a dishonest party. The risks presented by a spatially enhanced EAP-AKA procedure include:

- Unauthorized access from any IP network to the 3G network not prevented
- Subscriber impersonation with false geo-coordinates accepted at the 3G network
- False spatially augmented EAP-AKA requests originating from WLAN operator
- Successful tracking of attacker's real location eliminated

It is not feasible, for instance, for the 3G home network to retain location characteristics of potentially visited WLANs. If geo-coordinates describing WLANs are stored persistently at the home network, the 3G operator could determine the proximity of received geo-coordinates to those stored and known for a given WLAN. However, this is a very inefficient approach to securing a spatially enhanced EAP-AKA protocol.

For spatial control to be implemented successfully with the EAP-AKA protocol, attackers must be prevented from generating malicious or false authentication requests to the 3G network. Security mechanisms at the 3G home network and serving WLAN network should be implemented so that the integrity of authentication requests originating in WLANs can be determined. Falsified authentication requests should be identifiable to both the 3G home network and visited WLAN, and the 3G operator should be capable of assessing both the subscriber and the WLAN network. With positive verification of a EAP-AKA authentication request, access to rich 3G network resources can be granted. Conversely, with limited certainty as to the validity of an EAP-AKA authentication request, scaled down 3G network access can be granted. Spatially dependent EAP-AKA authentication requests become more secure as the 3G home network gains the capacity to measure the validity of each request. The interaction between 3G and WLAN networks must be used build the measure of trust held between parties. The 3G home network's vulnerability to false authentication requests generated from visited WLANs can be minimized with additional security procedures.

Securing 3G-WLAN User Authentication

3G-WLAN Trust Model

In a 3G-WLAN integrated network, it is essential that the parties involved build knowledge as to the behavior of the other participants. If relationships are defined between parties, the new integrated architecture and required authentication processes will be protected from potential abuse. To design a 3G-WLAN security solution, the trust relations between the home network, serving network and users must be identified. Two scenarios describe the trust relation between the home network and serving network. The home network may possess an existing relationship or agreement with the serving network and thus trusts the serving network. Otherwise, the serving network may not be trusted by the home network. It is essential in the latter case that the home network gains the capability of assessing a serving network to establish a trust relation. Maintaining an assessment of individual serving networks or an aggregate assessment of the operator of several serving networks will allow the 3G network to anticipate the quality of potential behavior of these otherwise unfamiliar networks. Requirements for interacting with a WLAN can then be aligned with the quality of trust the 3G operator possesses for the WLAN operator.

An established relation exists between the home network and mobile subscriber and this trust relation can be readily quantified by the home network. Referencing the subscriber's propensity for good behavior, a subscriber's proper adherence to rules or payment deadlines can be used to establish the trust level held for the subscriber by the home network. Assessing subscriber behavior strengthens security policies designed to prevent potential abuse of untested 3G-WLAN integrated networks. The home network can potentially distrust a subscriber since the subscriber can act fiendishly or someone has impersonated him or hijacked his/her session. Thus it is possible that the home network can not trust either the serving network or subscriber, when 3G network access is requested from an unfamiliar serving network. This scenario is resolved by both parties, serving network and subscriber, being required to obtain area coordinates used to build the user's area descriptors independently. The subscriber is not made aware of the spatial data sent to the home network on his behalf by the serving network. Thus the home network is protected with a successful authentication occurring only when the user's coordinate data matches that sent by the serving network. Thus, if either party, the serving network or subscriber, is dishonest concerning spatial data, authentication to the 3G network can not be completed.

Finally, the serving network may not readily trust the subscribers within an access network. If 802.11X user authentication is performed, a trust relation exists between the serving network and subscriber. However, user authentication is not performed in all WLAN access networks, primarily public networks where convenience of Internet access is extended to customers. Procedures can be implemented by serving networks so to gain confidence of subscribers honestly participating in the WLAN. Additionally, the home network must be confident of the validity of a subscriber's authentication request originating from within a WLAN. Gaining confidence of a subscriber's physical occupancy within a WLAN reduces the risks of 3G subscriber authentication requests being forged from the serving network. Gaining knowledge of a subscriber's behavior

while visiting a WLAN also allows the 3G home network to assess a subscriber's potential to commit or be thwarted into dishonest abuse of 3G service access.

Benefits of Ad-Hoc Serving Networks

In a WLAN with a traditional fixed network infrastructure, a one-to-many relationship is built between the WLAN operator and each mobile subscriber. Relationships are built independently between the serving network and each user and the occupants are unaware of other participant's activities or subscription level. However, assessing the behavior of mobile subscribers visiting serving networks is best built with *first-hand* knowledge obtained about subscribers. When a many-to-many relationship exists between subscribers, *first-hand* knowledge can be acquired from other WLAN participants observing and reporting information concerning their neighbors' behavior or attendance. This many-to-many structure requires an *ad-hoc* network design in which nodes are aware of others' communications and operate cooperatively to accomplish common networking tasks. Building secure relationships between 3G, WLAN network operators and subscribers is served by the establishment of *ad-hoc* networks implemented at WLANs. With subscribers aware of other's behavior or participation within a serving network, more knowledge can be gained by the home network to determine the trustworthiness of serving networks and the validity of user authentication requests.

With each subscriber providing observations in an *ad-hoc* serving network, a different localized trust model exists to define the level held by the serving network for each mobile subscriber. Relying on observations from one-hop neighbors, a subscriber can be trusted if k trusted nodes acknowledge the subscriber within a given time S_{Cert} [7]. This trust level can be refined further by weighing each of the k acknowledgements according to the trust level T assigned to each observer. An observer's trust level T can be revealed to neighbors through a certificate detailing the subscriber's trust level. Trust certificates built by a 3G operator must reflect each subscriber's historical good behavior and potential for future misbehavior. A process by which each subscriber's trust certificate is refreshed at the event of good or bad behavior and as well re-assessed at fixed time intervals is required to build robust and accurate trust levels for subscribers. A 3G network operator can calculate a base trust score based on the subscriber's credit score plus adherence to his/her payment schedule. Any misbehavior, possibly determined from public state records such as computer abuse or fraud, can be used to deduct from a subscriber's trust assessment. If a subscriber's equipment becomes prone to loss or theft, this vulnerability can be integrated into the quality of trust maintained by his/her provider. With limited subscriber history, a subscriber's trust certificate would initially start low, and would be incremented to reflect good behavior repeated over time. In an *ad-hoc* environment, mobile nodes will be required to advertise their trust certificate for the other participants either voluntarily or upon request.

Using the localized trust model for a *ad-hoc* serving networks in a 3G-WLAN integrated architecture, the presence of a mobile subscriber within a WLAN can be acknowledged by his neighbors. For instance, if each mobile node is required to periodically send a list of his/her neighbors to the serving network, the network can verify the presence of mobile subscribers within his network. The validity of neighbors' acknowledgements of WLAN participants can be further weighed according to the trust

certificate obtained from each neighbor. With each mobile subscriber MS_j possessing a trust level T_i of a real value between 0 ... 1 that is reporting on node MS_j , the trustworthiness of the set of acknowledgements becomes an aggregate of all the trust levels of the reporting nodes. For a set of k nodes $\{MS_1, MS_2, MS_3, MS_4, \dots MS_k\}$ reporting the participation of MS_j , the probability of MS_j residing in the serving network becomes

$$P = 1 - [(1 - T_1) * (1 - T_2) * (1 - T_3) \dots * (1 - T_k)]. \quad (3)$$

Thus, the higher the trust level of the reporting nodes, the more credible the report or evidence to the serving network of a mobile subscriber's presence.

Ad-hoc serving networks are beneficial to 3G-WLAN internetworking since the serving and 3G networks can gain acknowledgement of the parties participating in a given WLAN and the misbehavior of participating nodes can be detected. Poor behaving nodes may attempt to take advantage of the access controls set up within a WLAN in order to ultimately gain access to a 3G network. The risk of impersonation or false advertisement of a user's physical presence originating from a WLAN creates a threat to secure 3G network access. For instance, a group of dishonest users may attempt to feign the physical presence of another member by sending false acknowledgements of that member's participation. If a false advertisement of a user's WLAN participation is successful, an imposter may readily gain access to subscribed 3G services remotely. Thus, rigid access control within serving networks increases the overall security of integrated 3G-WLAN networks. Protocols within *ad-hoc* networks can be implemented by WLAN operators to identify impersonating or misbehaving nodes.

3G and Ad-Hoc WLAN Security Procedures

Authentication Acknowledgement

Serving networks employing an *ad-hoc* network infrastructure can play an active role in preventing dishonest authentication requests from reaching the 3G home network. The trustworthiness of a 3G subscriber's authentication request can be determined by the serving network if it requires that the request is acknowledged by k trusted observers from the WLAN. This mechanism would require all participant nodes overhearing an EAP-AKA identity response message relay that message back to the serving network. At the event of a mobile node's response to an EAP-AKA identity request, the serving network can assess the viability of the user's EAP-AKA response based on the set of acknowledgements received from neighboring nodes. The serving network can quantify the overall certainty of the user's EAP-AKA response by assessing the trust certificates attached to each observer's acknowledgement. Using threshold values R , for the number of acknowledgments received, and T , for the overall trust of the set of acknowledgements, the serving network can decide whether to forward the EAP-AKA authentication request for subscriber MS_j to the 3G home network. Thus, if k nodes $\{MS_1, MS_2, MS_3, \dots MS_k\}$ with trust certificates $\{T_1, T_2, T_3, \dots T_k\}$ acknowledge the authentication request of MS_j , if $k > R$ and

$$1 - [(1 - T_1) * (1 - T_2) * (1 - T_3) \dots * (1 - T_k)] > T \quad (4)$$

the serving network will forward the authentication request of node MS_j to the 3G home network. The trust level acquired for a user's authentication request and the set of acknowledgements can also be forwarded to the 3G home network upon request.

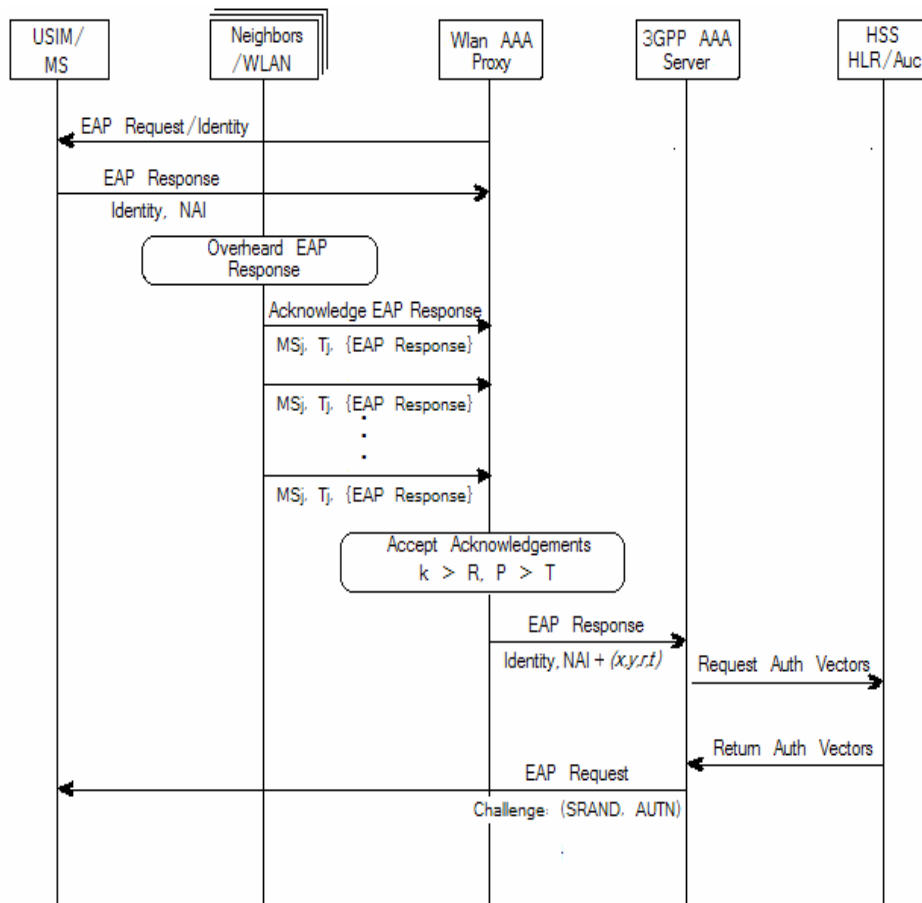


Figure 16 EAP-AKA Identity Response Acknowledgment

Figure 17 shows the best value for k to meet the threshold T , of overall trust of the set of acknowledgments, for increasing minimum trust levels T_j of the acknowledging nodes.

A potential vulnerability is presented when the serving network relies on a subset of participating node's acknowledgements for a subscriber's authentication request. If m dishonest nodes falsely acknowledge another member's 3G authentication request, and $m > R$, the serving network is reliant on those m nodes' false acknowledgements only. Honest nodes may not be aware of the m nodes' false acknowledgements and cannot warn the serving network of the nodes' dishonesty. Enforcing self-policing mechanisms involving all subscribers in a serving network can eliminate the potential for the m nodes' dishonesty from being hidden from the other nodes. A shared task between all members in a serving network can be enforced such as the building and maintaining a current participants list. With mutual-exclusive access to the list, each node would be required to update his entry by either adding his ID and timestamp or updating the timestamp for his entry. Applying the assertion that all nodes in the network are not dishonest, if an attempt is made to falsify the participants list, this misbehavior will be detectable by other nodes. The node updating the list would broadcast the new size of the

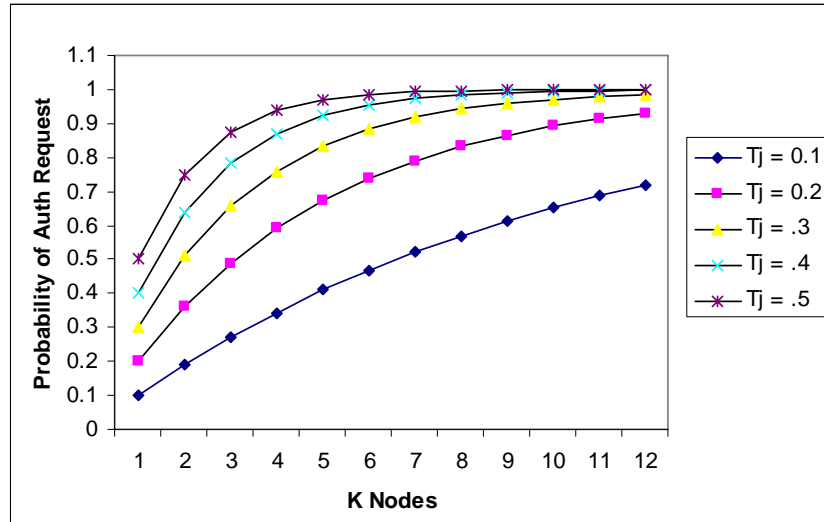


Figure 17 Acknowledgements Required for Trust Threshold T

list to all nodes and then forward the list to a chosen neighbor. Priority would be given to neighbors without an entry in the list and then to the neighbor whose entry is the oldest. Message looping would be prevented by bypassing those neighbors that possessed the list most recently. Adhering to rules to verify the validity of the participants list, a node receiving the list can report any discrepancy found to the serving network. Rules include verifying that the most recent timestamp belongs to the last possessing node or that the length of the list is only incremented or decremented by one entry at each interval. Verification of the shared participant's list prevents compromising nodes from interjecting false node IDs or timestamps into the list. Since the participants list is shared with all nodes, the list cannot be manipulated solely by the m dishonest nodes attempting to represent another dishonest party's attendance or 3G authentication request. The reporting node can notify the serving network of the previous node that possessed the list to identify corruption or misbehavior on that node's behalf. A range of corrective actions can be taken by the serving network to limit a questionable node's participation in the network or possibly deny network access completely. The serving network can notify the 3G home network of a node's misbehavior and request a verification of the misbehaving node's trust certificate. If the subscriber tampered with the certificate to include a false high trust level, the 3G home will be made aware of the subscriber's poor behavior.

Determining Trust in Serving Networks

In 3G-WLAN integration, the 3G operator must build robust trust assessments of the WLAN access networks potentially owned by different operators. The integration of 3G-WLAN networks requires that relationships between the 3G operators and WLAN serving networks be very well defined. The 3G home network must build an assessment per WLAN operator as to the potential of illegal 3G network access originating from that operator's wireless network. According to how well the 3G operator rates the trust relationship with a WLAN owner, the 3G home network can enforce varying security policies for carrying out EAP-AKA user authentication and granting network access. With a significant number of small unknown WLAN operators providing 3G networks access, maintaining a level of trust in an operator is critical to the 3G home network.

A means of assessing a serving network's proper operation and integrity must be obtainable to the 3G home network. Pre-existing relationships between 3G and WLAN operators, such as roaming agreements, would be the basis for initially quantifying the assessment of the 3G operator's trust for a WLAN network. If no relationship between a 3G and WLAN operator exists, the initial trust assessment must start low. A WLAN operator's historical security performance can be incorporated into his assessment so to protect the 3G network from becoming victim to malicious activity initiating from the WLAN. Integrating historical data of past DoS attacks, weak user authentication, privacy or poor security performance into the calculation of WLAN operator's trust level creates a realistic assessment for the operator. Similar to the trust relationship between a 3G operator and subscribers, the 3G operator's quantified trust value of a serving network would evolve over time and be re-assessed after significant events. Without mishap or breach of legal 3G network access originating from a serving network over extended time periods, the 3G home network's trust assessment of the serving network would increase to reflect the lack of potential vulnerability introduced to the home network by integrating with the WLAN.

Several approaches exist for the 3G network to obtain information about the integrity of a serving network of which it possesses limited trust. The *ad-hoc* serving network structure allows the 3G home network to gain access to information or events that occur at the serving network. By requesting additional information from the subscribers in a serving network, the 3G home network can gain insight into the serving network's performance. Particularly, at the event of an authentication request, the 3G home network can request acknowledgements from several authenticated subscribers or from a single, well trusted subscriber acting as a watchdog to verify the request from the new subscriber. The 3G home network can determine how reliable the serving network is at forwarding valid authentication requests on behalf of subscribers. To protect 3G services, when an EAP-AKA authentication request is received, the 3G home network can poll authenticated subscribers to verify a requestor's presence before proceeding with authentication.

By requesting acknowledgements from authenticated subscribers, a metric is established for the 3G home network to measure the level of trust, T_{SN} , for a serving network's security performance. With each authentication request acknowledged from subscribers in a WLAN, the 3G home network gains evidence of the proper functionality of a serving network. The potential that a serving network does not enforce policies to identify dishonest nodes and forwards fraudulent authentication requests becomes a threat to secure 3G network access. The risk also exists that a serving network AAA proxy may create fraudulent authentication requests on the behalf of dishonest parties. Acknowledging authentication requests from authenticated subscriber node's within a WLAN will minimize these threats posed to the 3G home network. By verifying the validity of authentication requests, the 3G network becomes less vulnerable to illegal access attempts initiated from the WLAN.

Overhead is introduced into 3G-WLAN internetworking as the level of trust held for a serving network is measured over time. With limited trust for a serving network's proper functionality, the number of requests by the 3G home network to acknowledge authentications would be at its highest. The overhead introduced is defined by the size of

the acknowledgment messages sent to the 3G home network and the number of messages requested by the home network for each authentication. Thus, if an acknowledgment contains an observing subscriber's identity and the acknowledged EAP identity response generated by a new subscriber, overhead of each authentication is equivalent to the size of the message, M , multiplied by the number of requests, N , made by the home network, or $N * \text{sizeof}(M)$. This overhead is incurred at each new authentication request originating from a visited WLAN and is ultimately dependent on the number of acknowledgements required by the home network. For serving networks with a low T_{SN} , certainty as to the validity of an authentication request is increased with a high value of N . Thus, the overhead incurred by subscribers in a poorly trusted WLAN will be the highest. The trust level held for a serving network, T_{SN} , can be incremented according to the number of successfully authentication requests positively acknowledged by subscribers in the visited WLAN. With subsequent successful authentications occurring for a serving network and a higher T_{SN} , the number of acknowledgements requested from the home network can be decreased. With the level of trust in a WLAN increasing, the incurred overhead by acknowledging subscribers will begin to diminish.

The range of values defining T_{SN} is configurable by the 3G operator as well as the metrics used to change the value of T_{SN} over time. For example, a 3G operator may determine that 100 acknowledged authentications are required in an average sized WLAN to increment T_{SN} , that ranges from 0 to 1, by .05 points. If a maximum number of 10 acknowledgements is required initially from the WLAN with a T_{SN} equal to 0, and the acknowledgement message size is 10 bytes, each authentication will add an initial 100 bytes of added data transmission on the part of the observing subscribers. As the total number of acknowledged authentications originating from a WLAN increases, T_{SN} will also increase. With higher trust in a serving network's integrity, the 3G operator may decrease the required number of acknowledgements requested for the WLAN as follows:

T_{SN}	Acknowledgements
$0 < T_{SN} < .30$	10
$.30 < T_{SN} < .50$	7
$.50 < T_{SN} < .70$	4
$.70 < T_{SN} < .80$	2
$.80 < T_{SN} < 1.0$	1

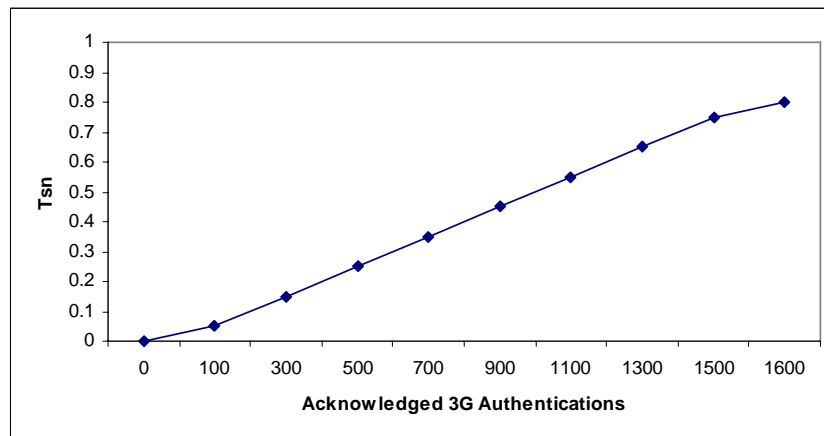


Figure 18 Increase of T_{SN} as Acknowledged Authentications Increase

Figure 18 demonstrates in this scenario how T_{SN} changes as the total number of acknowledged authentications increases over time. Figure 19 shows the reduction in overhead incurred by the observing subscribers as T_{SN} improves.

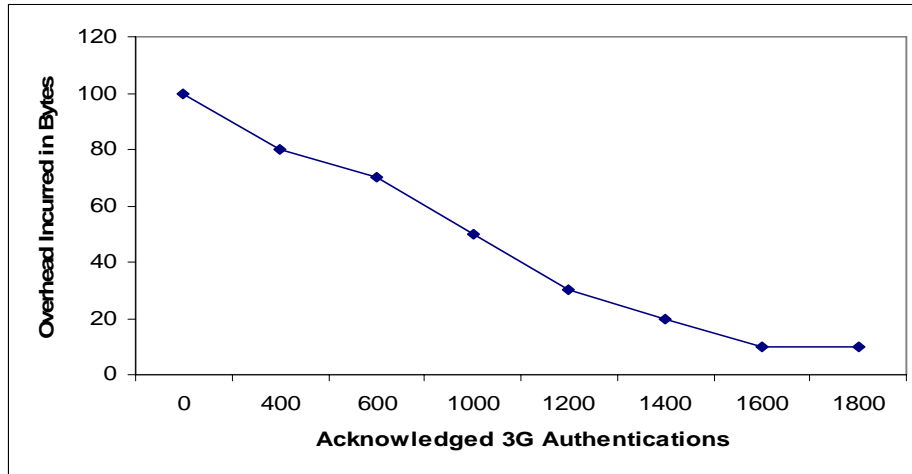


Figure 19 Overhead Decreases with Acknowledged Authentications

Conversely, if repeated invalid authentication requests originate from a serving network, the trust level held for the serving network will be decremented by the 3G operator. Any possible events that originate from a WAN that cause a negative impact on the 3G network should be well defined by the 3G operator and reflected in the level of trust for a WLAN. A denial of service attack initiated from a WLAN that prevents access to 3G services will be reflected in the 3G network’s trust assessment of the WLAN. Any abuse of a subscriber’s authentication credentials such as impersonation originating from a WLAN will impact that network’s trust level. If an attacker manipulates the 3G charging mechanism by interjecting excess packets at the WLAN the 3G network will act to protect itself from potential negative impact. According to the degree of severity of the impact to 3G network security, limited access to the 3G network can be granted and the 3G network can continue to request data from trusted, observing nodes in a WLAN.

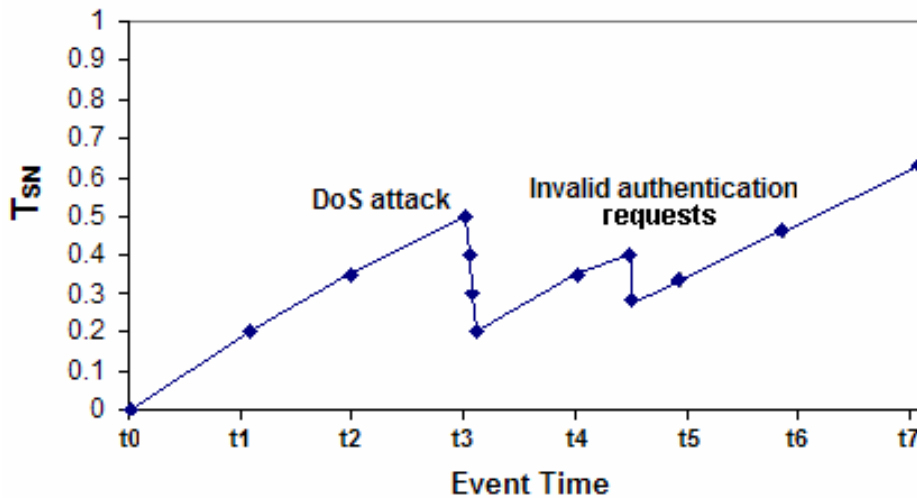


Figure 20 T_{SN} Decreases with Negative Events in WLAN

Figure 20 shows the impact of unacknowledged authentications occurring at a WLAN on that serving network's T_{SN} where at t_3 a DoS event drives the WLAN's T_{SN} down by .30 points and between t_4 and t_5 , repeated unacknowledged authentication requests drive T_{SN} down .15 points.

The 3G home network's acceptance of the data forwarded from a WLAN will be impacted by the trust certificates held by the forwarding subscribers. For instance, if subscribers MS_A and MS_B , with trust levels T_A and T_B , are polled by the 3G home network as to the presence of node MS_C , the 3G home network can accept the observer's reports if the aggregate trust of the observing nodes is greater than the acceptable threshold T_W , or $1 - [(1 - T_A) * (1 - T_B)] > T_W$. With deficient aggregate trust for the information received from a serving network, authentication requests can be denied from the 3G network or access to only limited 3G services can be granted. Trust levels for both subscribers, T_A and T_B , and the serving network, T_{SN} , must be considered when the 3G home network analyzes the acknowledgements obtained. So, if T_{Auth} is the home network's minimum required certainty that the authentication request was issued from the serving network and

$$1 - [(1 - T_A) * (1 - T_B) * (1 - T_{SN})] > T_{Auth} \quad (5)$$

an authentication vector for MS_C can be sent to the serving network. Figure 1d shows the required level of trust in observing nodes for serving network of differing trust levels, T_{SN} , needed to gain the overall certainty, T_{Auth} , for a valid authentication request. By building an assessment of trust for serving networks, the 3G home network can protect itself from lax or dishonest serving network proxies. If the serving network voluntarily notifies the 3G home network of misbehavior occurring in the WLAN, the decrement of trust assessment for the serving network should not be as severe. The 3G home network can continue to monitor the behavior of serving networks until a threshold of trust is reached and initiate methods to minimize fraudulent network access originating from serving networks.

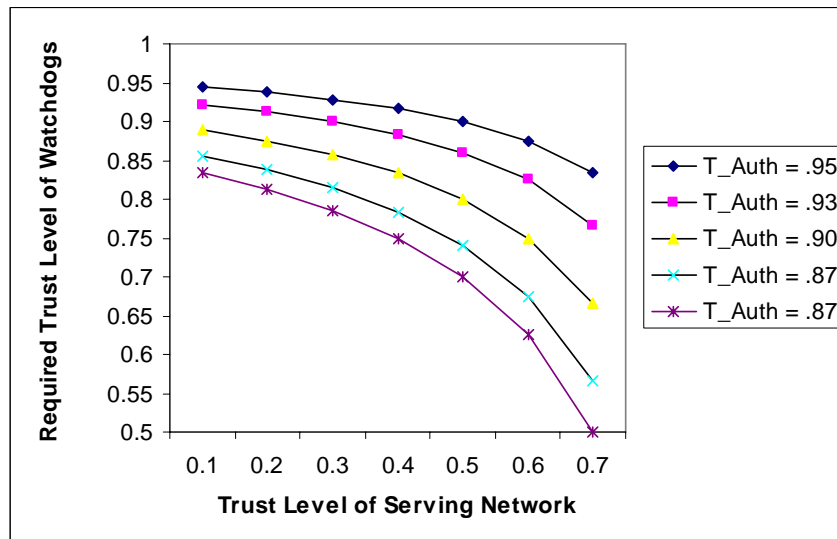


Figure 21 Required Trust in Observing Nodes for T_{SN}

Illegal access to the 3G home network from a visited WLAN can also be identified if a communication path is enforced between a 3G AAA server and VLR/SGSN for each location area. If a AAA server queries the VLR/SGSN as to the active status of a subscriber within the location area in which a serving network resides, invalid EAP-AKA authentication requests can be detected. Thus, a one-to-one relationship should exist between an AAA server and location area or VLR/SGSN. A restriction can be placed on EAP-AKA initiated authentication requests in that a 3G subscriber must currently be authenticated via the radio access network and be active within the location area in which a visited WLAN resides. This methodology provides a verification method for the 3G home network to determine the validity of EAP-AKA authentication requests. If an authentication request originates from a serving WLAN network which is not contained within a subscriber's active location area, the 3G network can consider the request invalid and thus adjust the serving network's trust assessment. A decreased trust assessment would reflect the possible dishonesty of the serving network or the potential for the serving network AAA proxy to be manipulated from an outside malicious party to generate false authentication requests. This communication path enforced between a 3G AAA server and VLR/SGSN is most warranted when additional subscribers are not present in a visited WLAN to acknowledge the authentication request of a new subscriber. An initial check by the 3G AAA server that a user is active within the VLR/SGSN location area in which the WLAN resides is a precautionary method that can protect the 3G home network. Otherwise, the 3G network can implement steps to protect itself from the potentially malicious network access.

Protecting 3G Network Services

Precautions can be taken by the 3G operator when granting network access to subscribers in a WLAN in which an insufficient trust relationship has been established. Added security procedures and restrictions on service access can be used to minimize the possible abuse of 3G network access. Threat of abuse of 3G network services increases with the level of services and access offered to visitors of unknown wireless LANs. Potential guards to protect the 3G home network include:

- further encrypting user authentication challenge
- limiting the number of subscriber connections from a WLAN
- limiting service suite accessible from a WLAN

Additional encryption of an authentication challenge sent via EAP-AKA transport to a non-trusted serving network can further protect the 3G network from intrusion. Advanced encryption can be accomplished by the 3G home network by XORing an authentication challenge with the user's equipment serial number, PIN or password. This additional protection of subscriber authentication vectors protects the 3G network from the vulnerability of subscriber impersonation. The authentication and key management field, AMF, appended to the network authentication value, AUTN, used by the subscriber equipment to authenticate the 3G network, can be set to indicate to the user that additional encryption has been exercised. This approach is highly beneficial when the 3G home network interacts with a WLAN in which no existing relationship or trust index has been determined. With no pre-existing trust for a newly visited WLAN, the 3G home network's determination of the credibility of authentication requests becomes dependent

on the input of other subscribers. If no other authenticated subscriber is present in the WLAN, a sole subscriber can not be authenticated. Rather than denying subscriber authentication, the 3G home network can execute additional encryption protecting its services and the subscriber. The 3G home network may also enforce a quota on the concurrent subscriber connections allowed from a visited WLAN to mitigate potential network access abuse. Additional attribute value pairs defined for the DIAMETER capabilities exchange can define the *size* of a serving network based on its capacity or total possible number of user connections.

Further protection of the 3G network resources can be implemented by limiting the types of services accessible from visited WLANs. Limiting access to rich multimedia services will protect the 3G network from abuse, while access to simple services, such as text based messaging and limited Internet access, can be maintained to provide basic functionality to subscribers. Access to different classes of services can be assigned to subscribers within a WLAN according to the trust level held for the WLAN operator or according to the level of certainty held by the 3G home network of a subscriber's valid authentication request. Voice, data and multimedia services are classed into four groups by 3GPP according to the level of bandwidth required and the sensitivity of the content to delay in delivery or re-transmission. Background services include minimal bandwidth to provide e-mail, text messaging and limited downloads while interactive services allow larger downloads for video or files, web browsing and potential server access such as to database servers. Streaming services emerging for wireless customers include streaming video or music on demand and webcasts. These services are delay sensitive, require prioritization to deliver continuous content and require significant bandwidth. Voice over IP, VoIP, and interactive conferencing or video are emerging streaming services for mobile customers. The final 3GPP service class is the conversational class for voice or video telephony. With services categorized into these classes, access to each class of service can be granted according to rules set by the 3G home network. For instance, for WLANs in which the 3G home network possesses only 30% of allowable trust level, T_{SN} , access to background and traditional telephony services can be provided. For trust levels ranging between 30% and 60%, interactive services access can be granted, while for WLANs in which the 3G home network possess above 60% certainty of operational integrity and valid user authentication, premium streaming services can be made accessible. Providing access to premium 3G services is a benefit for WLAN operators that can increase their overall number of clientele and market reach. Thus, granting tiered service access to WLAN serving networks builds motivation for operators to build strong trust relationships with 3G networks and minimize any potential abuse that could originate from their network.

Conclusion

Focus on converging 3G and IP technologies has centered on the integration of 3G and wireless LAN networks. High-speed 3G data service can be delivered to customers through WLAN networks giving customers more mobility and access to critical data. Standards have been defined to secure an efficient means of allowing seamless 3G service access from WLAN serving networks. Architectural options have been defined to connect 3G and WLAN networks either through dual network hardware or through the transport of 3G services over the IP network. All aspects of 3G subscriber management, including authentication, must be accurately implemented for the successful deployment of 3G-WLAN integrated networks. In hybrid 3G-WLAN networks, securing 3G user authentication initiated from a WLAN is particularly crucial. The 3G home network must be protected from forged authentication requests and unauthorized access. Dishonest WLANs or those vulnerable to outside malicious parties attempting to manipulate the hybrid 3G-WLAN environment to gain illegal 3G network access must be identified and thwarted.

3G-WLAN integrated networks can be secured by the implementation of *ad-hoc* network architecture in visited WLANs. By gaining access to subscriber's observations within a serving network, both the serving network and 3G home network can enforce policies to reveal dishonest participants. Steps can be taken to measure the level of dishonest activity occurring in a serving network and to mitigate abuse of 3G network access. For instance, serving networks can act as firewalls on the behalf of 3G networks filtering incredible authentication requests not acknowledged properly from observing WLAN participants. Authentication procedures can be further strengthened by information forwarded to the 3G home network on behalf of a subscriber by the serving network or other trusted subscribers present. Spatial control of 3G user authentication can be implemented so to bind user authentication to the WLAN he/she is currently residing in. With limited authority to verify a subscriber's accurate location within a WLAN beyond the range of the subscriber's current location area, LA, the 3G home network becomes reliant on serving networks to send valid authentication requests and user spatial data. Thus, robust trust relationships must be strictly defined and maintained between 3G operators and potentially visited WLANs. Subscriber authentication can be made contingent on the level of trust held by the 3G home network for the visited serving network and the certainty of the subscriber's presence at the WLAN. Proper performance and repeated successful authentication requests originating from the WLAN will deem the serving network as a trusted partner in the hybrid 3G-WLAN network.

References

- [1] “3GPP Technical Specifications Group Core Network and Terminals: Numbering, Addressing and Identification”, TS 23.003 V6.7.0, 3GPP, 2005
- [2] “3GPP Technical Specification Group Services and System Aspects: Specification of the Milenage Algorithm Set”, TS 35.206 V6.0.0, 3GPP, 2004
- [3] Apostolis K. Salkintzis, Chad Fors, Rajesh Pazhyannur, “WLAN-GPRS Integration for Next-Generation Mobile Data Networks”, IEEE Wireless Communications, October 2002
- [4] Imad Aad, “The IEEE 802.11 Standard”, IN’Tech, May 31, 2002
- [5] Geir M. Koiem, Thomas Haslestad, “Security Aspects of 3G-WLAN Internetworking”, IEEE Communications Magazine, November 2003
- [6] Geir M Koiem, Vladimir A Oleshchuk, “Spatio-Temporal Exposure Control”, IEEE International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings, IEEE, 2003
- [7] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, “Self-securing Ad Hoc Wireless Networks”, UCLA Computer Science Department
- [8] Jyh-Cheng Chen, Ming-Chia Jiang, and Yi-Wenn Liu, “Wireless LAN Security and 802.11i”, IEEE Wireless Communications, February 2005
- [9] Kalle Ahmavaara, Henry Haerinen, Roman Pichna, “Internetworking Architecture Between 3GPP and WLAN Systems”, IEEE Communications Magazine, November 2003
- [10] Kui Ren, Tiejian Li, Zhiguo Wan, Feng Bao, Robert Deng, Kwangjo Kim, “Highly reliable trust establishment scheme in ad hoc networks”, Computer Networks, 2004
- [11] P. Eronen, T Hiller, Glen Zorn, “AAA Working Group RFC 4072: Diameter Extensible Authentication Protocol EAP Application”, The Internet Society, August 2005
- [12] Pat Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko, “AAA Working Group Internet Draft: Diameter Base Protocol”, draft-ietf-aaa-diameter-17.txt, The Internet Society, December 2002
- [13] Pat Calhoun, Bernard Aboba, Erik Guttman, Dave Mitton, Dave Nelson, Juergen Schoenwaelder, Barney Wolff, Lixia Zhang, “AAA Working Group Internet Draft: AAA Problem Statements”, The Internet Society, January 2002
- [14] Sumit Kasera, Nishit Narang, 3G Mobile Networks – Architecture, Protocols and Procedures, McGraw-Hill, 2004

[15] William Arbaugh, Narendar Shankar, Y. C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", University of Maryland, March 30, 2001

Vita

Lyn Evans is a systems science graduate student at Louisiana State University. Her technical focus is on security for software development and wireless communications. Her professional experience includes real time software development and support for defense and commercial applications. She intends to work professionally to develop remote secure access for database applications after graduation.