

# Secure authentication in heterogeneous wireless networks

Arjan Durresi<sup>a,\*</sup>, Mimoza Durresi<sup>a</sup> and Leonard Barolli<sup>b</sup>

<sup>a</sup>*Indiana University Purdue University, 723 W. Michigan St. SL 280M, Indianapolis, IN 46202, USA*

<sup>b</sup>*Fukuoka Institute of Technology, 3-30-1 Wajiro-Higashi, Higashi-ku, Fukuoka 811-0295, Japan*

**Abstract.** The convergence of cellular and IP technologies has pushed the integration of 3G and WLAN networks to the forefront. Gaining secure access to 3G services from 802.11 WLANs is a primary challenge for this new integrated wireless technology. 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 visited WLAN.

With limited capacity to determine a user's location only to within a current cell and restrictions on accessing users' location due to privacy, 3G operators must rely on spatial data sent from visited WLANs to implement spatial authentication control. A potential risk is presented to 3G operators since no prior relationship or trust may exist with a WLAN owner. Algorithms to quantify the trust between all parties of 3G-WLAN integrated networks are presented to further secure user authentication. Ad-hoc serving networks and the trust relationships established between mobile users are explored to define stronger algorithms for 3G-WLAN user authentication.

## 1. Introduction

Mobility is a 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 improve by utilizing the capacity of the IP backbone to deliver rich user data.

The challenges presented by the convergence of these the two networks are readily being addressed to facilitate the successful implementation of new mobile technology. Each network has been enhanced to provide 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. Challenges exist in that security protocols in the respective IP and 3G networks are not compatible in architecture

---

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

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 for 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.

The rest of this paper is organized as follows: Section 2 presents some related background and describes the risks of spatial control in EAP-AKA protocol. Section 3 presents our proposed trust model and trust relationships to secure users. Section 4 concludes.

## 2. Background

Global technical consortiums have been formed to address the technical requirements and define specifications for emerging 3G technologies. The 3<sup>rd</sup> generation partnership project, 3GPP, has defined 6 scenarios for integrating 3G and WLAN networks [15]. 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 [15]. These options define a *tight coupling* and *loose coupling* methodology for combined networking functionality.

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 standards and ensure interoperability between these different new networks [10]. 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].

*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 [15]. 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 [4].

*3G-WLAN Security Architecture:* 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 [11]. 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 visits a WLAN [1]. 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 [7,9]. 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 [6].

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. 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 and unauthorized access to 3G user data.

The 3G home network can not readily trust visited WLANs and the possibility for malformed EAP-AKA authentication requests originating from vulnerable WLAN AAA proxies becomes a threat. For authentication requests originating and received from an IP network, the 3G home networks must do more to verify the authenticity of that request. An attacker can successfully impersonate a valid user if he possesses knowledge of a user's IMSI and subscriber key,  $K_i$ , and can gain access to the user's 3G services and potential sensitive information.

*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 efficacy of spatially controlled user authentication increases as unique subareas 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 breeched 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, subscriber impersonation with false geo-coordinates, false spatially augmented EAP-AKA requests originating from WLAN operator and a successful tracking of attacker's real location eliminated. 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.

### 3. Securing 3G-WLAN user authentication

#### 3.1. 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 gain 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.

### 3.2. 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  $S_{Cert}$  [13]. 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.

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  $MS_i$  possessing a trust level  $T_i$  (a real value between 0 and 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  $\{MS_1, MS_2 \dots MS_k\}$  reporting the participation of  $MS_j$ , the probability of  $MS_j$  residing in the serving network becomes

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

Thus, the higher the trust levels 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.

### 3.3. 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  $\{MS_1, MS_2, \dots MS_k\}$  with trust certificates  $\{T_1, T_2, \dots T_k\}$  acknowledge the authentication request of  $MS_j$ , if  $k > R$  and

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

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 1 shows the best value for  $k$  to meet the threshold  $T$ , of overall trust of the set of acknowledgements, 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

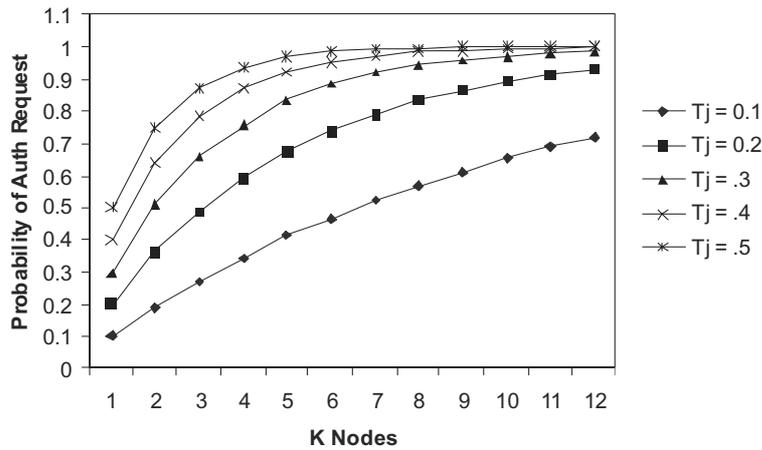


Fig. 1. Acknowledgements required for trust threshold  $T$ .

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 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 who's 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 malicious behaviour.

### 3.4. 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 interoperability 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 potentially providing 3G networks access, quantifying and maintaining a level of trust in an operator becomes 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

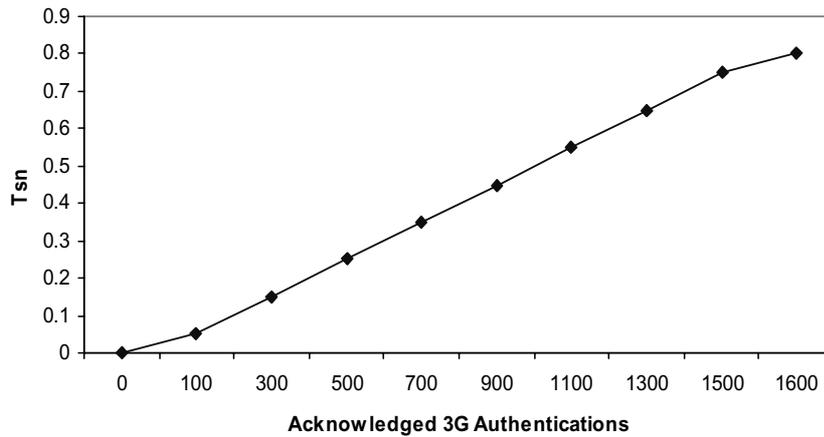


Fig. 2.  $T_{SN}$  increases as acknowledged authentications increase.

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  $N * M$ .

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. 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.

Figure 2 demonstrates in this scenario how  $T_{SN}$  changes as the total number of acknowledged authentications increases over time. Figure 3 shows the reduction in overhead incurred by the observing subscribers as  $T_{SN}$  improves.

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

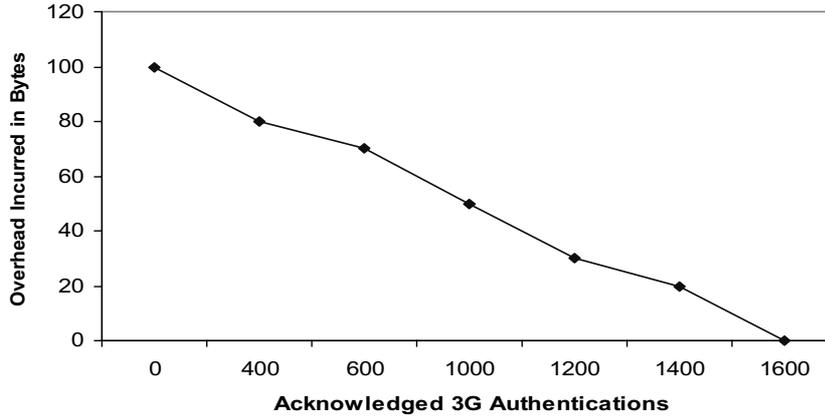


Fig. 3. Overhead decreases with acknowledged authentications.

from a WAN that causes 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 4 shows the impact of unacknowledged authentications occurring at a WLAN on that serving network's TSN where at  $t_3$  a DoS event drives the WLAN's TSN down and between  $t_4$  and  $t_5$ , repeated unacknowledged authentication requests drive TSN down.

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 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

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

an authentication vector for  $MS_C$  can be sent to the serving network. Figure 5 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

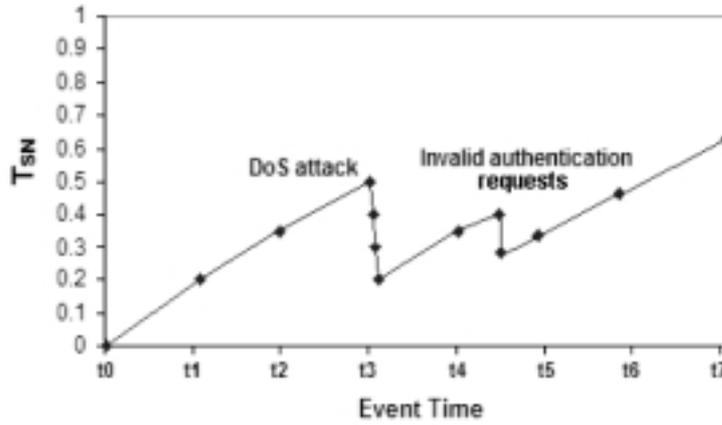


Fig. 4.  $T_{SN}$  decreases with negative events in WLAN.

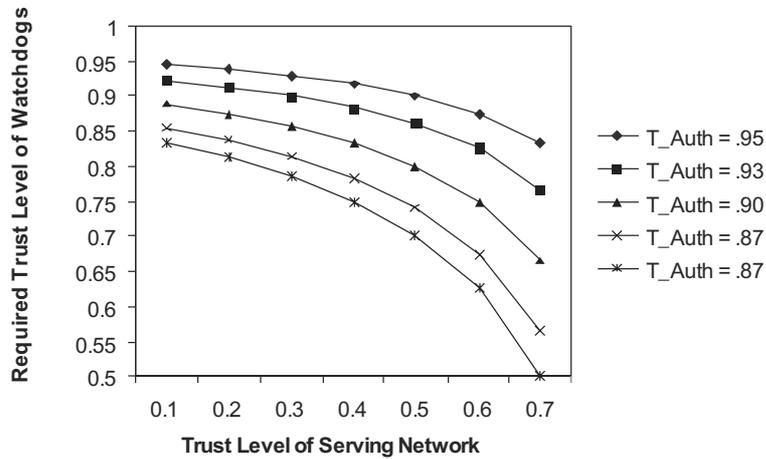


Fig. 5. Required trust in observing nodes for  $T_{SN}$ .

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.

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 an 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

servicing network's trust assessment. A decreased trust assessment would reflect the possible dishonesty of the servicing network or the potential for the servicing 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.

#### 4. Conclusions

In hybrid 3G-WLAN networks, securing 3G user authentication initiated from a WLAN is particularly crucial. Steps must be taken to protect the 3G home network from forged authentication requests. 3G network access must be restricted to within the WLAN of which an authentication request was received. WLANs vulnerable to outside malicious parties or attempting to manipulate the hybrid 3G-WLAN environment to gain illegal 3G network access must be identified and thwarted.

By strictly defining and maintaining trust relationships between all parties in a 3G-WLAN integrated network, authentication procedures are strengthened. Subscriber authentication and access can be made contingent on the level of trust held by the 3G home network for the visited serving network. Serving networks can act as firewalls on the behalf of 3G networks filtering incredible authentication requests not acknowledged properly from observing WLAN participants. With repeated proper performance and successful authentication requests, a servicing network can be deemed a trusted partner in a 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] I. Aad, The IEEE 802.11 Standard, IN'Tech, May 31, 2002/.
- [4] K. Ahmavaara, H. Haerinen and R. Pichna, Internetworking Architecture between 3GPP and WLAN Systems, *IEEE Communications Magazine* **41**(11) (November 2003), 74–81.
- [5] W. Arbaugh, N. Shankar and Y.C.J. Wan, *802.11 Wireless Network has No Clothes*, University of Maryland, March 30, 2001.
- [6] P. Calhoun, B. Aboba, E. Guttman, D. Mitton, D. Nelson, J. Schoenwaelder, B. Wolff and L. Zhang, *AAA Working Group Internet Draft: AAA Problem Statements*, The Internet Society, January 2002.
- [7] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, *AAA Working Group Internet Draft: Diameter Base Protocol*, draft-ietf-aaa-diameter-17.txt, The Internet Society, December 2002.
- [8] J.-C. Chen, M.-C. Jiang and Y.-W. Liu, Wireless LAN Security and 802.11i, *IEEE Wireless Communications* **12**(1) (February 2005), 27–36.
- [9] P. Eronen, T. Hiller and G. Zorn, AAA Working Group RFC 4072: Diameter Extensible Authentication Protocol EAP Application, The Internet Society, August 2005.
- [10] S. Kasera and N. Narang, *3G Mobile Networks – Architecture, Protocols and Procedures*, McGraw-Hill, 2004.
- [11] G.M. Koiem and T. Haslestad, Security Aspects of 3G-WLAN Internetworking, *IEEE Communications Magazine* **41**(11) (November 2003), 82–88.
- [12] G.M. Koiem and V.A. Oleshchuk, Spatio-Temporal Exposure Control, IEEE International Symposium on Personal, *Indoor and Mobile Radio Communications Proceedings PIMRC 2003* **3** (September 2003), 2760–2764.
- [13] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, *Self-securing Ad Hoc Wireless Networks*, UCLA Computer Science Department.

- [14] K. Ren, T. Li, Z. Wan, F. Bao, R. Deng and K. Kim, *Highly reliable trust establishment scheme in ad hoc networks*, Computer Networks, 2004.
- [15] A. K. Salkintzis, C. Fors and R. Pazhyannur, WLAN-GPRS Integration for Next-Generation Mobile Data Networks, *IEEE Wireless Communications* (October 2002), 112–124.

---

**Arjan Durresi** received his B.E., M.E. and Ph.D. (all summa cum laude) in Electronics and Telecommunications, in 1986, 1991 and 1993, respectively; and a Diploma of Superior Specialization in Telecommunications from La Sapienza University in Rome, Italy and Italian Telecommunications Institute. He is currently with the Department of Computer and Information Science at Indiana University Purdue University at Indianapolis. Previously he held roles as Research Scientist of Computer Science and as Adjunct Professor of Electrical and Computer Engineering at The Ohio State University. His current research interests include network architectures, heterogeneous wireless networks, security, QoS routing protocols, traffic management, optical and satellite networks, and bioinformatics. Dr. Durresi has authored more than fifty journal papers, and more than eighty conference papers. He is an area editor for the Ad Hoc Networks Journal. He is the founder and co-founder of several workshops, including the IEEE International Workshops on Heterogeneous Wireless Networks – HWISE, the International Workshop on Advances in Information Security – WAIS, and the IEEE International Workshop on Bio Computing. Dr. Durresi has chaired and co-chaired several conferences and workshops, including the 20th IEEE AINA-2006.

**Mimoza Durresi** received the B.E. in Electronic-Telecommunications in 1989 at Tirana University, a Diploma of Superior Specialization in Telecommunications from La Sapienza University in Rome, Italy and Italian Telecommunications Institute in 1991. She received the MS in Electric Computer Engineering in 2002 from The Ohio State University and the Ph.D. in Computer Engineering from Fukuoka Institute of Technology in 2006. She teaches at Indiana University Purdue University at Indianapolis. Previously she was with Franklin University. Her research interest are in wireless networking, inter vehicle communications and routing.

**Leonard Barolli** received BE and PhD degrees from Tirana University and Yamagata University in 1989 and 1997, respectively. From April 1997 to March 1999, he was a JSPS Post Doctor Fellow Researcher at Department of Electrical and Information Engineering, Yamagata University. From April 1999 to March 2002, he worked as a Research Associate at the Department of Public Policy and Social Studies, Yamagata University. From April 2002 to March 2003, he was an Assistant Professor at Department of Computer Science, Saitama Institute of Technology (SIT). From April 2003 to March 2005, he was an Associate Professor and presently is a Full Professor, at Department of Information and Communication Engineering, Fukuoka Institute of Technology (FIT). Dr. Barolli has published more than 200 papers in referred Journals and International Conference proceedings. He was an Editor of the IPSJ Journal and has served as a Guest Editor for many International Journals. Dr. Barolli has been a PC Member of many International Conferences and was the PC Chair of IEEE AINA-2004 and IEEE ICPADS-2005. He was General Co-Chair of IEEE AINA-2006, Workshops Chair of iiWAS-2006/MoMM-2006, Workshop Co-Chair of ARES-2007 and IEEE AINA-2007. Presently, he is General Co-Chair of IEEE AINA-2008, Workshop Chair of iiWAS-2007/MoMM-2007, and Workshop Co-Chair of ARES-2008. Dr. Barolli is the Steering Committee Chair of CISIS International Conference and is serving as Steering Committee Member in many International Conferences. He is organizers of many International Workshops. His research interests include network traffic control, fuzzy control, genetic algorithms, agent-based systems, wireless networks, ad-hoc networks and sensor networks. He is a member of SOFT, IPSJ, and IEEE.



# Hindawi

Submit your manuscripts at  
<http://www.hindawi.com>

