Mobile Distributed Authentication Protocol

A. F. Al Shahri, D. G. Smith and J. M. Irvine
Dept. of Electronic & Electrical Engineering
University of Strathclyde, Glasgow, G1 1XW, UK
aied@comms.eee.strath.ac.uk, d.g.smith@eee.strath.ac.uk, j.m.irvine@strath.ac.uk

Abstract - Networks access control is a crucial topic and authentication is a pre-requisite of that process. Most existing authentication protocols (for example that used in the GSM mobile network) are centralised. Depending on a single entity is undesirable as it has security, trust and availability issues. This paper proposes a new protocol, GSM-Secure Network Access Protocol (G-SNAP). In G-SNAP, the authentication procedure and the network access control is handled by a quorum of authentication centres. The advantages of the novel protocol include increased security, availability and a distributed trust.

I. Introduction

Authentication represents the front door of any secure system. Strong authentication protocols are needed to restrict network access to only authorised users. Most existing authentication protocols are centralised, using a single authentication centre. These centralised approaches suffer certain drawbacks such as an attack on that single entity compromises the whole system and if that entity becomes unavailable then authorised users are unable to access the system. In addition trust is focussed on that single entity which becomes unconditionally trusted, resulting in increased risk and it may not be suitable for the more complex business models in 3G systems. Secret sharing schemes and quorum systems are tools to increase security and availability and to distribute trust between entities [1]. The basic idea of secret sharing is to divide a secret into pieces called shares. Thereafter, the pieces are distributed amongst users such that the pooled shares of specific subsets of users allow reconstruction of the original secret [2]. Non-qualified subsets have absolutely no information on the secret. Secret sharing schemes are useful in any important action that requires the concurrence of several designated entities to be initiated [3].

A quorum system for a system of nodes is a collection of subsets (quorums) of nodes, each pair of which has a non-empty intersection. Each quorum can act on behalf of the system. For example, let U be a set of nodes, $U = \{a, b, c, d\}$. Then $Q = \{\{a, b\}, \{b, c\}\}$ is a quorum set under U. The intersection property enforces consistency between nodes, which is important in replicated objects and for node co-ordination. Quorum systems [4] have been used for a number of applications in the area of distributed systems including mutual exclusion protocols, replicated data protocols, database access control protocols and multi-party computations. In this paper a new protocol, GSM Secure Network Access Protocol (G-SNAP) is proposed. This protocol is based on secret sharing schemes, which have a quorum access structure. Section II introduces authentication in GSM networks. Section III describes the proposed protocol G-SNAP. Section IV provides analysis and simulation results. A comparison between G-SNAP and centralised approaches is discussed in Section V.

II. Authentication in GSM Networks

In GSM, authentication is achieved by checking the validity of a subscriber's SIM card. An authentication algorithm (termed A3) is stored on the SIM card and also in the authentication centre (AuC) on the network. The process is challenge-response based. The A3 algorithm uses two input parameters: the secret key, Ki, which is stored in the SIM card and in the network, and a random number (RAND), which is transmitted to the mobile station as a challenge. The A3 algorithm uses Ki and RAND to calculate a response (SRES). The mobile station will send back the SRES to the network as a response to the challenge. The network uses the same RAND, Ki, and A3 to produce an SRES, which is checked against the response from the mobile station [5].

A. Drawbacks

- A challenge-response procedure such as GSM uses is a strong authentication process to access network resources. The major drawback of the GSM authentication process comes from its centralised nature. The authentication centre in the network controls the authentication, and as such, if the authentication centre is attacked or compromised, then unauthorised users may obtain access to network resources.

- A centralised system also has availability issues. Authorised users will be unable to obtain access if that entity breaks down, denying service to users.

- A final concern is one of trust. In GSM networks, the authentication centre is unconditionally trusted. Such a centralised trust model is not recommended, as focussing the trust on a single entity will increase the risk, which might affect the system security.

- The communication between all users and the central authentication node involves a lot of signalling traffic and high load on the authentication node.

III. G-SNAP

G-SNAP is an extension of recently developed protocol called a secure network access protocol (SNAP) [6]. The proposed G-SNAP algorithm seeks to address GSM centralised authentication deficiencies by using a distributed approach. G-SNAP makes use of both secret sharing and quorum structures, which have previously been used in security applications to increase security and availability [7, 8].

In order, to perform authentication or access control in a GSM network using G-SNAP, the mobile station contacts a quorum of authentication centres with a quorum size *k* to obtain permission. Fig. 1 depicts the mobile distributed model. Each member of the quorum participates in the authentication process by identifying the user and providing the corresponding share required to complete the authentication process. At the same time none of the quorum members can handle the whole authentication or grant network access on its own. In other words, the authentication process is distributed between all the quorum members. However, fewer than *k* nodes (authentication centres) cannot grant the network access. If one of the authentication centres becomes uncontactable, the mobile station, after a certain time can contact another quorum to obtain the secret shares and hence it can access the network resources. Hence to increase availability, G-SNAP assumes that the mobile station can contact *l* quorums. The selection of *k* and *l* is a trade-off between increased security and minimised overhead. In G-SNAP, the first (local) authentication server (local AuC) which receives the mobile station signal will start the authentication process. The local AuC participates in the negotiation but does not control or take the network access decision on its own. Fig. 2 depicts the required signalling for the user to obtain the required shares from a quorum of *k* AuC's. The G-SNAP works as follows:

1. Once the local AuC receives a signal from the *ms* to register or to use the network.
2. The local AuC will ask the *ms* to obtain permission or to be authenticated by a quorum of AuCs by providing *k* shares (*S1,..Sk*) from any quorum.
3. The *ms* will start independently communicating with the AuCs, which are already known by the SIM card of that *ms* or given by the local AuC, and ask for the corresponding shares. If *ms* does not receive a response from one AuC in a certain time it will try another quorum, up to *l* quorums.
4. Each AuC will check if the *ms* is authorised and then will send the corresponding share if appropriate
5. After receiving the required *k* shares by the SIM card of the *ms*, the *ms* will send the concatenated secret shares as one message to the local AuC.
6. The local AuC will reconstruct the AC using a reconstruction function. If it is correct, it will give the *ms* permission to access the network or alternatively output a rejection message.

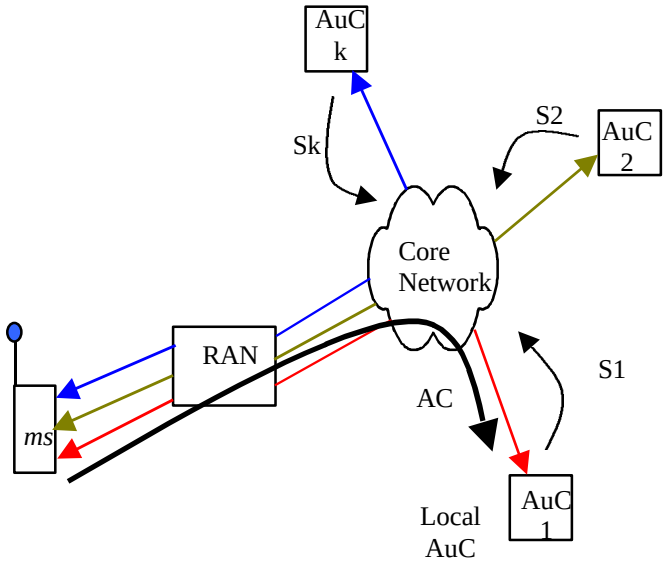

Fig. 1 The distributed authentication infrastructure

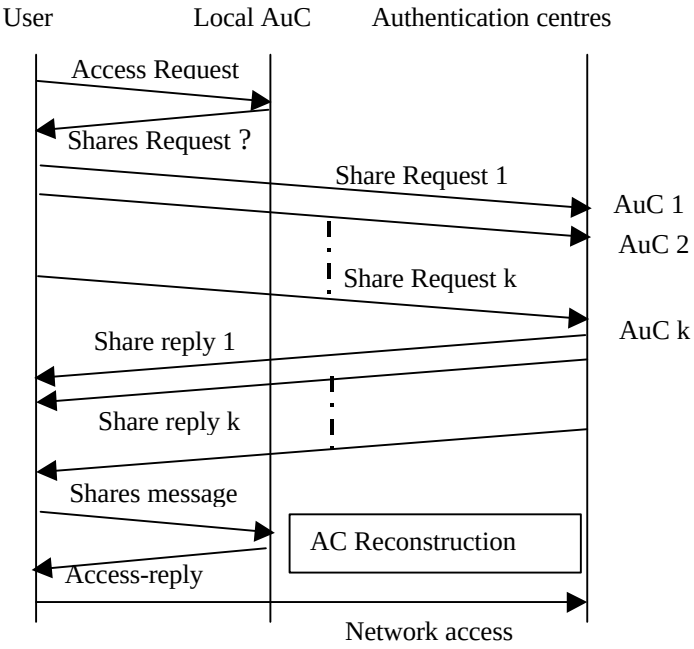

Fig. 2: G-SNAP signalling

IV. Simulation analysis

It is important to model the performance of any new protocol before its implementation. Most security protocols have been evaluated from a security and information theory perspective only. Networks are the main platform for most of the applications including security applications. These protocols use the networks to convey the messages between the protocol components. Therefore, it is important to evaluate

the performance of the protocol, using metrics such as delay, efficiency and resilience and to analyse their impact on users. G-SNAP is developed to increase security, availability and to distribute trust. In this paper G-SNAP has been studied using simulations based on network simulator version 2 (NS-2) [9]. The delay experienced by users using G-SNAP or centralised approaches is obtained. In addition a comparison between SNAP and centralised authentication protocols is investigated

The simulation model involves two main steps:

- The network is loaded by generating background traffic to load all the links.
- After a certain time, whenever the network has been loaded, G-SNAP traffic will start generating the authentication packets.

In GSM networks the AuCs are connected to the mobile switching centres (MSCs). All the MSCs are in the core network and are linked by a fixed network. The G-SNAP architecture is illustrated in Fig. 3. In order to study the performance of G-SNAP, an arbitrary core network of 7 MSC nodes is built as shown in Fig. 4 using NS-2. Fig. 4 depicts the topology of the authentication nodes using a quorum system. For example, Q3 contains three member nodes 0, 4 and 5. As shown in Table 1, there are four quorums and each authentication node is a member of two quorums. The user allocation to local quorums is shown in the same Table. In this quorum system the quorum size *k* is 3. The signalling link capacity between nodes is 1 MB/s and the link delay is 10 ms. Each node contacts its neighbour using a full duplex link. In this simulation each node represents an authentication centre in the MSC.

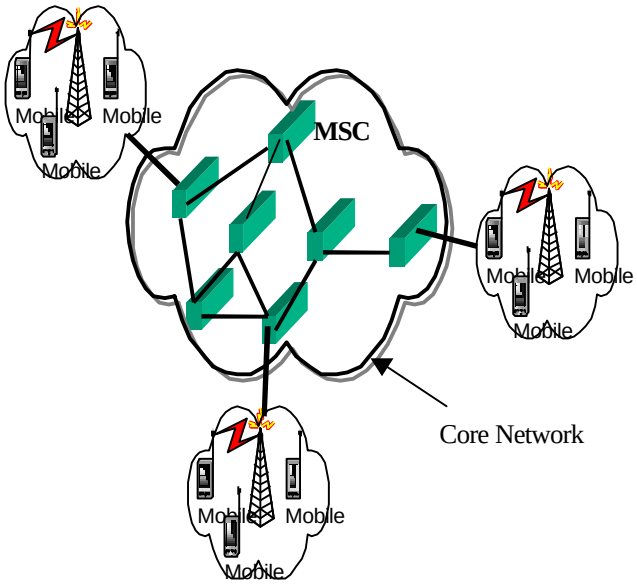

Fig. 3 G-SNAP architecture.

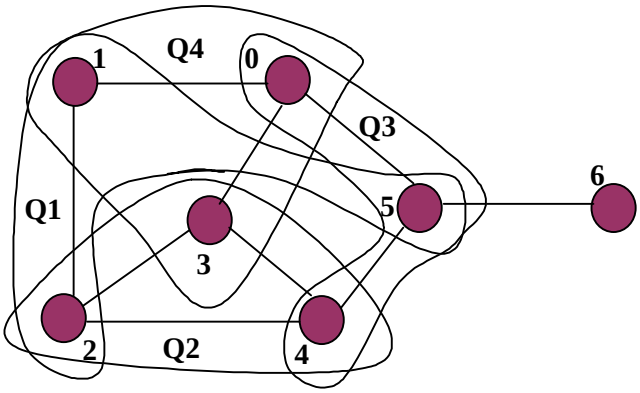

Fig. 4 Network topology

TABLE I
Quorum system

Quorum number	Quorum members	User allocation
Q1	1, 2, 5	1
Q2	2, 3, 4	2,3,4
Q3	0, 4, 5	5,6
Q4	0, 1, 3	0

A. *Assumptions*

- To generate the background traffic, UDP agents are used. Both source and destination nodes use UDP agents.
- The background traffic is exponentially distributed traffic with packet size 500 bytes.
- For G-SNAP traffic ping agents are used in both the source and destination nodes. Using the ping agent we can calculate the round trip time delay between source and destination.
- The authentication packet size is assumed to be 250 bytes [6].
- The authentication processing time is not considered in this study.
- The quorum size *k* is 3

B. *Simulation results*

To improve the statistical significance of the results, the simulation was run for a large number of cycles. It is assumed that each node represents an authentication centre The user will send a packet that contains the required information for the user to identify themselves to the other nodes. In this case we assume that the authentication packet is large enough to handle all the needed information. The packet size is 256 bytes. Using G-SNAP, the user will simultaneously send *k* packets to the authentication nodes. The selection of the routing path is based on the built-in routing protocol provided by ns-2. Since ping agents are used, packets will go back directly after reaching the destination towards the source. In G-SNAP the user needs to

wait for the last packet to arrive such that the waiting time does not exceed the predefined time limit. In order to compare G-SNAP with centralised approaches, three scenarios have been considered.

In the first one, centralised users contact a centralised authentication server (CAS) in node 2. G-SNAP users will contact one of the quorums. Q2 is selected. This means that each user should contact the quorum's members which are node 2, 3 and node 4. Fig. 5 shows the average delay experienced by users in both cases. It can be observed from that figure the following:

- Users 1 and 2 will experience an increased delay using G-SNAP.
- All other users will have exactly the same delay.

In the second scenario, G-SNAP users will contact local quorums as shown in Table I. The centralised node is node 2 as before. The results are shown in Fig. 6. It appears that G-SNAP performs better in this case. Users 0, 5 and 6 experienced smaller delay using G-SNAP compared to the centralised approach. The location of the centralised node with respect to users is a major issue.

In the third scenario, G-SNAP users will contact local quorums and the centralised users will contact node 6. It can be observed from Fig. 7 that G-SNAP is more efficient than contacting a remote centralised node.

If we study these results we come up with the following observations:

1. The delay increases if the number of hops between nodes is increased.
2. In most of the cases some users will experience exactly the same delay, either using a centralised authentication centre or using G-SNAP (although traffic load will increase).
3. The location of the authentication node with respect to the user has a direct impact on results in both centralised and distributed approaches.
4. Designing an efficient quorum system and distributing the users on local quorums is crucial and can lead to good results.

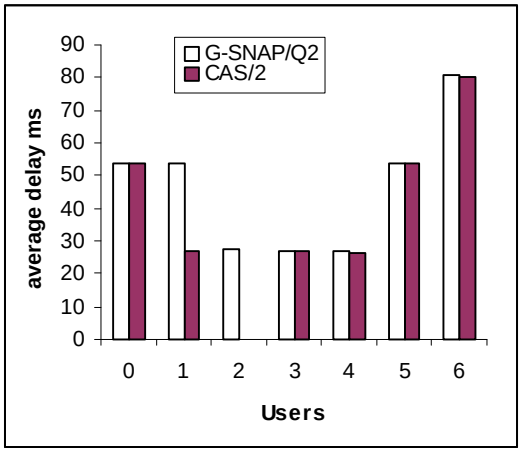

Fig. 5 G-SNAP on Q2 and CAS on node 2

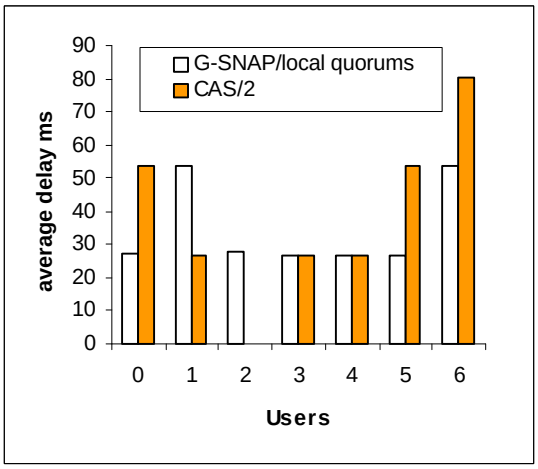

Fig. 6 G-SNAP on local quorums CAS on node 2

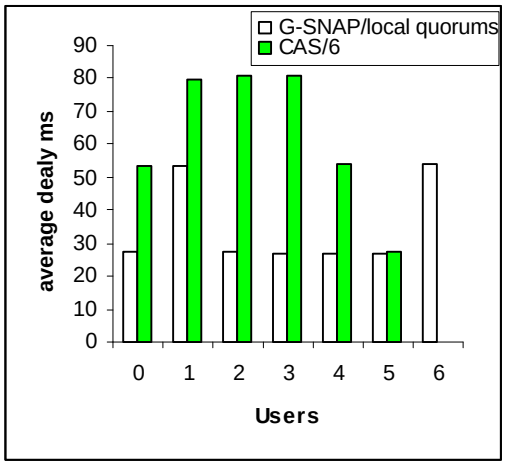

Fig. 7 G-SNAP on local quorums CAS on node 2

V. Discussion

In this discussion a comparison between G-SNAP and centralised approaches is investigated. In order to determine the signalling overhead caused by G-SNAP, the number of messages sent to the authentication nodes is required. In G-SNAP the user must contact *k* nodes to collect the required shares. Hence, signalling overhead is increased by *k* compared to centralised approaches. Contacting the local AuC is not considered in the signalling overhead since it is not significant. In centralised approaches all users contact a single node increasing the traffic destined for that node. At the same time the load on the single entity will be high. In contrast G-SNAP distributes the load to the quorums. If there are *l* quorums then the load to each quorum is equal the total load divided by *l*. G-SNAP can achieve load balancing as well. G-SNAP overcomes the drawbacks of centralised approaches as mentioned in section II. G-SNAP increases

security since the user needs to be authenticated by a quorum of nodes. In addition, if one node is compromised, the attacker will only receive one share, so the system as a whole remains secure. In the centralised case, a successful attack on the authentication centre will compromise the entire system. Furthermore, G-SNAP increases the availability too, if one node or quorum is unavailable the user can contact another quorum. Additionally, G-SNAP distributes the trust among the quorum members and none of the quorum nodes can grant or control access on its own. In high security applications the advantages of G-SNAP would appear to outweigh the additional signalling overhead.

VI. Conclusion

There is a need to have multiparty authentication protocols such that more than one server controls the authentication process. This results in increased security and availability, and also distributed trust, which overcomes the centralised authentication approaches deficiencies. The importance of this will increase with 3G networks, which are more distributed in nature and have more complex business arrangements. G-SNAP is a new protocol, which achieves these objectives. The performance evaluation of G-SNAP compared to centralised approaches is discussed in this paper. Although G-SNAP does introduce more signalling, the delay impact on users is marginal. G-SNAP can be more efficient than the centralised approach if it is used to provide more localised distributed authentication.

References

[1] A. F. Al Shahri, D. G. Smith and J. M. Irvine, “Implementation of quorum systems to increase network security”, PGNET 2002, June 2002, Liverpol University, UK.

[2] A. F. Al Shahri, D. G. Smith and J. M. Irvine, “Implementation of Secret Sharing to Increase Network Security and Reliability,” ESPRC Postgraduate Research in Electronics and Photonics (PREP), April 2002, Nottingham University, UK.

[3] G. J. Simmons. “An introduction to shared secret and/or shared control schemes and their application,” In Contemporary Cryptology, The Science of Information Integrity, pages 441-497. IEEE Press, 1992.

[4] Malkhi, “Quorum systems,” chapter in the encyclopaedia of distributed computing march 1999

[5] J. Dunlop, D. Girma and J. Irvine, *Digital Mobile Ccommunications and the TETRA System*, John Wiley & Sons. 1999.

[6] A. F. Al Shahri, D. G. Smith and J. M. Irvine, “A Secure network access protocol (SNAP),” unpublished.

[7] L. Gong. “Increasing availability and security of an authentication service,” IEEE J. Selected Areas Comm., 11(5):657-662, 1993.

[8] M. Naor and A. Wool. “Access control and Signatures via quorum secret sharing,” In Proc. 3rd ACM Conf. Comp. And comm. Security, pages 157-168, New Delhi, India, Mar. 1996.

[9] Network Simulator version 2 (NS-2) UC Berkeley, USA, http:// www.isi.edu/nsnam/na/ns-documentation.