NEXT GENERATION NETWORKING 2011

Multi-Service Network Workshop

7-8 July 2011, Cosener's House, Abingdon, UK

Mobility, AAA, Security, Privacy : How can we support Real-World Network Mobility?

Panagiotis Georgopoulos

panos@comp.lancs.ac.uk
http://www.comp.lancs.ac.uk/~georgopp/

School of Computing & Communications
Lancaster University

Joint work with Dr. Ben McCarthy, Dr. Chris Edwards

Analyzing the Title…

Mobility, AAA, Security, Privacy :
How can we support Real-World Network Mobility?

- Mobility : How can we allow network mobility protocols to operate efficiently in real-world Mobile Network deployments?
- AAA : How can we provide a practical and scalable AAA infrastructure to facilitate the requirements of both Mobile Networks and the Access Networks they get connectivity from?
- Security : How can we provide secure network access and secure data transmission for Mobile Networks and their Nodes?
- Privacy : How can we disclose the identity of the Mobile Network from each Access Network it connects to?

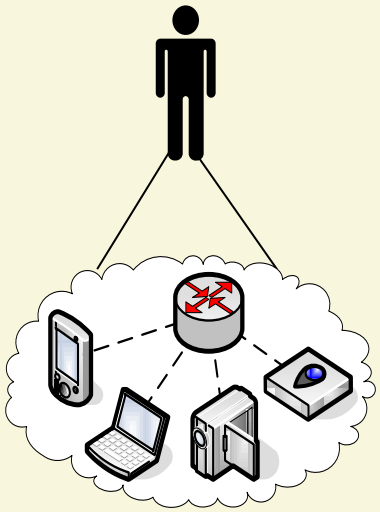
What is a Mobile Network ?

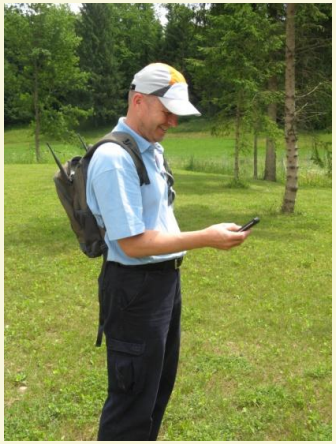
- Mobile Network (MN) is a group of mobile devices requiring networking support (mainly Internet connectivity) that moves as a whole
  - In contrast with a mobile host (e.g. a user with a laptop) that moves individually

- Characteristics :
  - Mobile Network Nodes (the MN's devices) remain relatively immobile in relation to one another
  - A Mobile Router (MR) is responsible to provide seamless mobility for all the devices in the network without them having to run any extra protocols or be aware of their mobility

Mobile Network examples

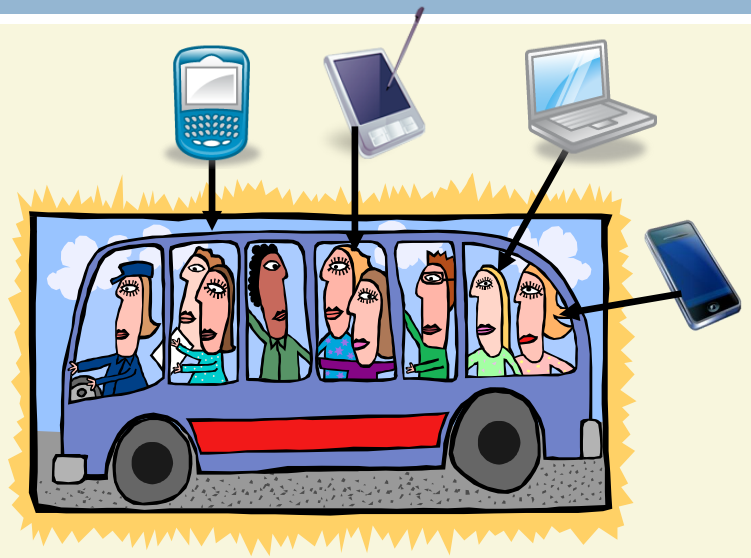
- Public Transportation (Buses, Trains, Coaches, Airplanes)
- Emergency Forces (Police, Fire Brigade, S&R Teams)
- PANs / VANs (Consumer Electronics)





A real-life scenario with a Mobile Network

- A bus company decides to offer Internet connectivity to passengers that board its buses every day.



- As the bus does its every-day route through town, its MR is responsible to obtain Internet connectivity from various publically available AN's Access Points being sporadically located around town, and share it to the passengers' devices by projecting a wireless hotspot in the bus.

What does a Mobile Network require ?

- Motivation -

Mobility

Uninterrupted Connectivity (seamless mobility) for all the MNNs whilst the bus changes is point of attachment from one Access Network to another (thus changing its IP)

AAA

- Dynamic Trust establishment between AN & the MN (*mutual authentication*)
- Quick, effortless and secure network access to each AN (*the MR should avoid to be configured with the different type of credentials each protocol and AN requires*)

Security

Secure data transmission both locally, in the vicinity of the hotspot the MR provides to its MNNs, but also globally, as its MNNs' data are transmitted from the MN to the Internet via the AN

Privacy

Avoid revealing the identity of the MR of the MN to each AN as it roams (for privacy purposes)

What does an Access Network require ?

- Motivation -

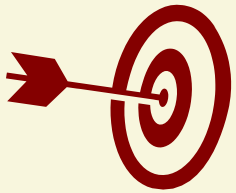
AAA

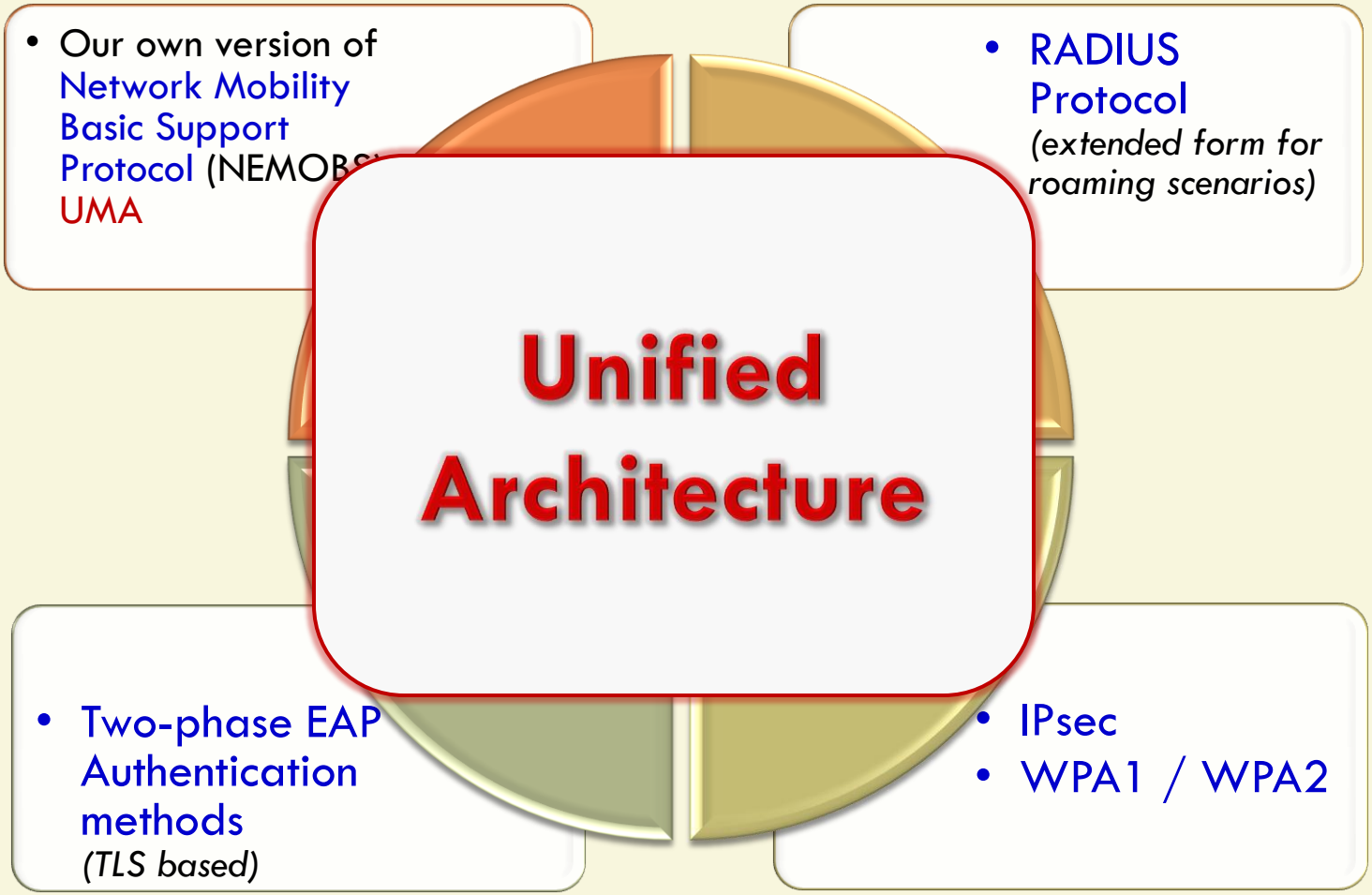
- A robust, efficient and well configured AAA service to :
  - Authenticate the Mobile Router of the Mobile Network in a practical and scalable manner (*it is unrealistic to expect that each AN should know in advance each MR requesting network access on behalf of a MN*)
  - Authorize access based on ISP specific policies
  - Account for the MR's access and bill the MN later (financial benefits)

Security

Avoid compromising the AN's security policies and disallow unauthorized access to Mobile Networks

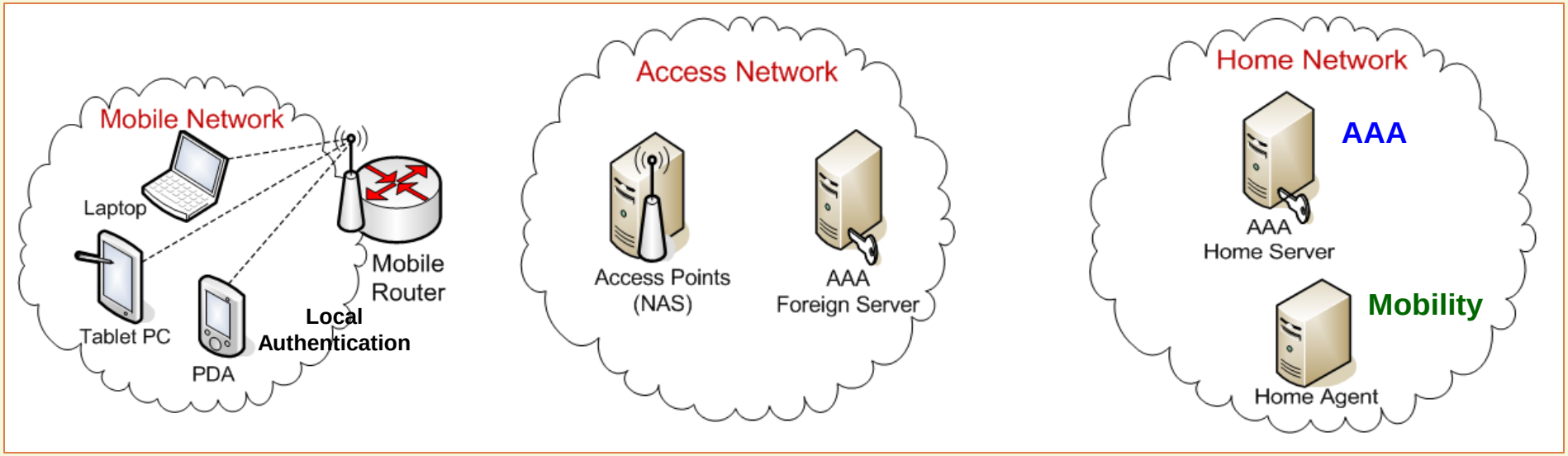
Mapping Requirements to Protocols
- a standards based approach -





Our Unified Architecture (UA)

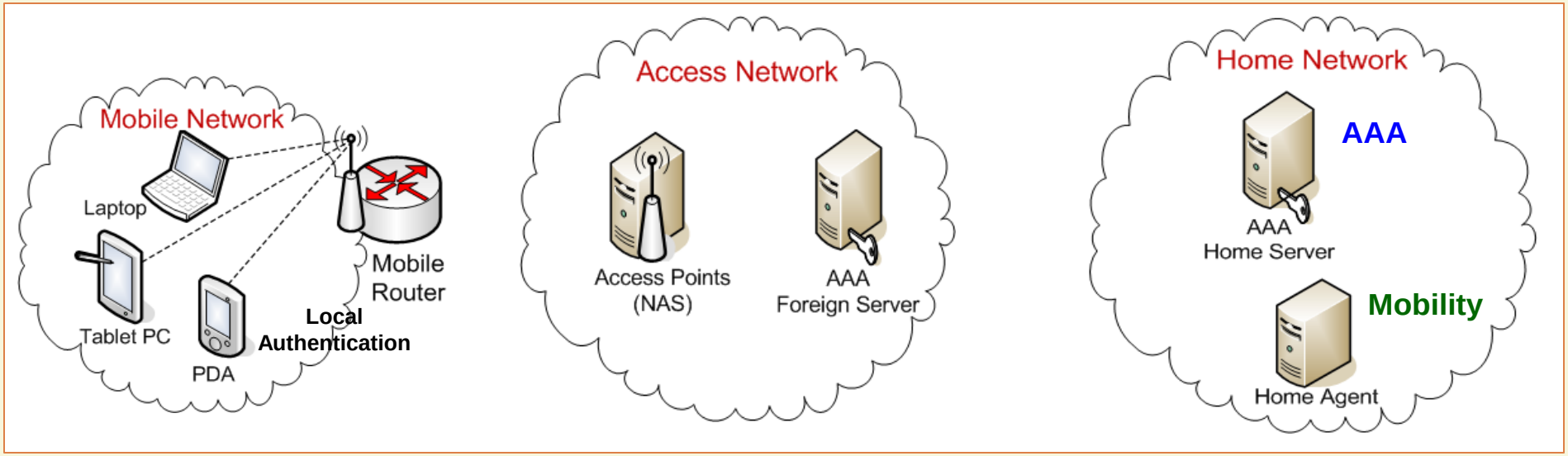
- bridging the gap between Mobility and AAA -



- Overlay the AAA model in its extended form over NEMO BS' Architecture and integrated the Mobility & AAA services in a unified, seamless and secure way
- Three entities : Home Network, Access Network , Mobile Network
- The MR is responsible to provide the Mobility and AAA services for the whole network
  - Authenticate the whole network to ANs
  - Local Authentication of the MNNs
    - Advantages : when the MN roams, the MNNs might notice a slight disruption in the service but they don't need to be reauthenticated (no need to send packets to a remote AAA server (saving bandwidth & minimizing delays)

Our Unified Architecture (UA)

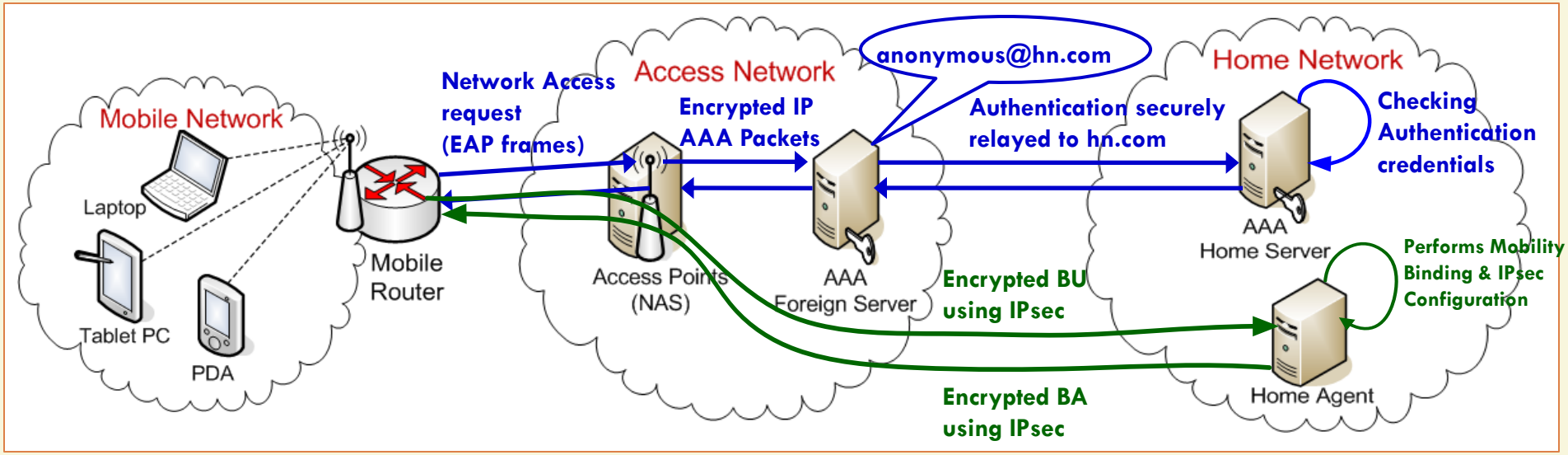
- bridging the gap between Mobility and AAA -



- Our Unified Architecture does not alter neither augment the design of the AN : ready for today's Internet infrastructure ✓
- UA requires a Service Level Agreement between the AN and the HN : AN can relay the authentication procedure to the HN
  - No need for all the small scale networks to get SLAs, a hierarchical model with intermediate proxy AAA servers can be supported
- Advantages of this collaborative design : ✓
  - The AN doesn't need to have any configuration for the MN / The HN already has authentication credentials for the MN
  - Dynamic trust establishment of the MR and the AP
  - Both AN and HN have incentives to join the collaborative scheme
  - The identity of the MR is not revealed (privacy is kept) because a two phase EAP authentication method

Our Unified Architecture (UA)

- how does the MN become fully operational when roaming ? -



- Fully operational in three Phases :
  - **Phase 1 :** Layer 2 Association : Connects to the Access Point
  - **Phase 2 (AAA) :** Layer 2 & 3 AAA Communication and WiFi Security Configuration
  - **Phase 3 (Mobility) :** Layer 3 Mobility & IPsec configuration

Qualitative Evaluation

- satisfying the requirements of the MN -

- UA bridges the gap between Mobility and AAA in a secure and efficient way and satisfies the requirements of both the Mobile Network and the Access Network.

- Our UA satisfies the following requirements of the MN :

  1. Secure, unobtrusive and trouble-free network access :
     - The MR does not need to be configured with the different types of credentials each visiting AN requires.
     - The MR does not reveal its identity to each AN it is visiting, thus keeping its privacy whilst roaming.
     - Dynamic trust establishment between the MR and the AN.

  2. Secure transmission of data locally, in the range of the AP using WPA/WPA2, and globally, as data leave the AN and travel to the Internet using IPsec.

  3. Constant and reliable connectivity is provided with the use of UMA, which in conjunction with the trouble-free network access that is provided using the AAA service, leads to seamless and quick roaming for the MN.

Qualitative Evaluation

- satisfying the requirements of the AN -

- Our UA satisfies the following requirements of the AN:

  1. Authentication of the MR without requiring to have information about it in advance.

  2. Authorization of the MR according to its local policies.

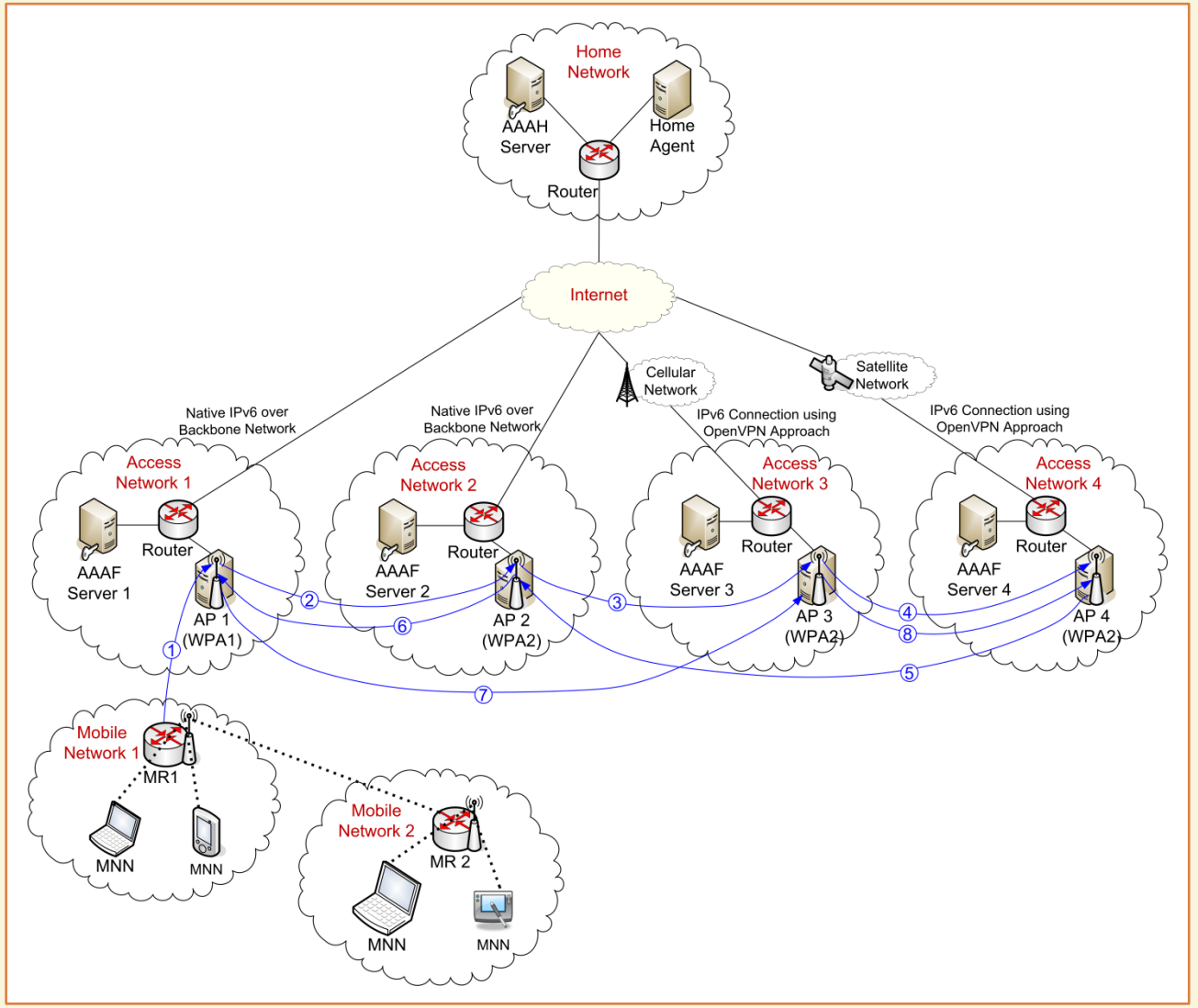
  3. Accounting of the MR for its MNNs' network use in order to bill its HN for the provided service.

  4. All the previous transactions are performed without compromising the security policies of the AN and by inducing financial benefits.

Quantitative Evaluation

- IPv6 Live Testbed -

- IPv6 Testbed to allow us to experiment with different network configurations and routes.
- Different type of Links : Native IPv6 Link, 3G Link and Satellite Link evaluate the suitability and applicability of our approach.
- Live Testbed mimicking exactly how communication would take place in an actual deployment scenarios. Our tests present real-time traffic characteristics over the Internet.
- We perform hundreds of Roamings and we focus on how quickly the MNNs become fully operational using different authentication methods (EAP-TLS, EAP-TTLS).



Results : EAP-TTLS Tests

- EAP-TTLS : Authentication of the Client (MR) with a username/password combination
- Profiled thoroughly each timing of each Roaming of each Phase
- Two very important features for roaming scenarios :
  - WPA2 PMKSA Caching
  - Reduces roaming timings from 13.5sec to 0.037sec & #packets from 21 to 4
  - AAA Session Resumption
  - Reduces roaming timings from 2.4sec to 0.792sec & #of packets from 21 to 11

Test 1 : EAP-TTLS without Session Resumption

Phases \ Roamings	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.126	2.088	1.153	1.723	1.960	1.184	1.706	1.606
Phase 2 (sec.)	0.222	0.158	2.441	13.502	0.010	0.229	0.009	0.037
Phase 3 (sec.)	1.630	1.770	2.110	5.454	1.854	2.141	1.734	3.720
Total (sec.) :	2.978	4.016	5.704	20.679	3.824	3.554	3.449	5.363

Test 2 : EAP-TTLS with Session Resumption

Phases \ Roamings	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.136	1.210	1.754	1.932	1.754	1.242	1.651	1.970
Phase 2 (sec.)	0.359	0.035	0.792	4.376	0.014	0.062	0.014	0.015
Phase 3 (sec.)	1.474	2.069	2.228	4.340	2.672	2.012	2.836	5.100
Total (sec.) :	2.969	3.314	4.774	10.648	4.440	3.316	4.501	7.085

Number of Packets transmitted for each Roaming

#Packets	TEST 1	TEST 2
Stage 1	7/16	7/16
Stage 2	5/16	5/6
Stage 3	5/16	5/6
Stage 4	5/16	5/6
Stage 5	4/0	4/0
Stage 6	7/16	7/6
Stage 7	4/0	4/0
Stage 8	4/0	4/0

Results : EAP-TTLS Tests

P. Georgopoulos, B. McCarthy and C. Edwards "*A Collaborative AAA Architecture to Enable Secure Real-World Network Mobility*" In: 10th International Conference on Networking (Networking 2011), 09-13 May 2011, Valencia, Spain

- Overall conclusion is that the MN becomes fully operational within a few seconds (4 sec w/o SR, 3.2 sec with SR)
- PMKSA Caching and Session Resumption improved the results significantly when applicable
- Our current work improves these even further (60%-70% further reduction)

Test 1 : EAP-TTLS without Session Resumption

Phases \ Roamings	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.126	2.088	1.153	1.723	1.960	1.184	1.706	1.606
Phase 2 (sec.)	0.222	0.158	2.441	13.502	0.010	0.229	0.009	0.037
Phase 3 (sec.)	1.630	1.770	2.110	5.454	1.854	2.141	1.734	3.720
Total (sec.) :	2.978	4.016	5.704	20.679	3.824	3.554	3.449	5.363

Test 2 : EAP-TTLS with Session Resumption

Phases \ Roamings	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.136	1.210	1.754	1.932	1.754	1.242	1.651	1.970
Phase 2 (sec.)	0.359	0.035	0.792	4.376	0.014	0.062	0.014	0.015
Phase 3 (sec.)	1.474	2.069	2.228	4.340	2.672	2.012	2.836	5.100
Total (sec.) :	2.969	3.314	4.774	10.648	4.440	3.316	4.501	7.085

Number of Packets transmitted for each Roaming

#Packets	TEST 1	TEST 2
Stage 1	7/16	7/16
Stage 2	5/16	5/6
Stage 3	5/16	5/6
Stage 4	5/16	5/6
Stage 5	4/0	4/0
Stage 6	7/16	7/6
Stage 7	4/0	4/0
Stage 8	4/0	4/0

Results : EAP-TLS Tests

- EAP-TLS : Authentication with Certificates for both the Client and the Server
- EAP-TLS presented similar results with EAP-TTLS, albeit transmitted more packets
- Again, PMKSA and SR improved the results significantly

Test 1 : EAP-TLS without Session Resumption

Roamings / Phases	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.302	1.585	1.394	1.520	1.324	1.384	2.160	1.450
Phase 2 (sec.)	0.414	0.184	2.011	12.908	0.011	0.461	0.009	0.016
Phase 3 (sec.)	2.126	2.352	3.180	5.100	2.474	2.806	3.024	4.012
Total (sec.) :	3.842	4.121	6.585	19.528	3.809	4.651	5.193	5.478

Test 2 : EAP-TLS with Session Resumption

Roamings / Phases	First Associations				Subsequent Associations			
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
Phase 1 (sec.)	1.357	1.596	1.242	1.350	1.106	1.148	1.346	1.408
Phase 2 (sec.)	0.425	0.039	0.606	4.314	0.013	0.049	0.010	0.011
Phase 3 (sec.)	2.033	2.334	2.622	3.891	2.108	2.890	2.946	3.289
Total (sec.) :	3.815	3.969	4.470	9.555	3.227	4.087	4.302	4.708

Number of Packets transmitted for each Roaming

#Packets	TEST 3	TEST 4
Stage 1	7/14	7/16
Stage 2	5/14	5/6
Stage 3	5/14	5/6
Stage 4	5/14	5/6
Stage 5	4/0	4/0
Stage 6	7/14	7/6
Stage 7	4/0	4/0
Stage 8	4/0	4/0

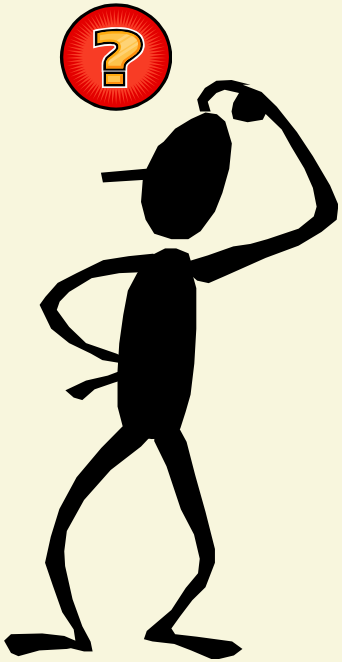
Conclusion

- We presented a Unified Architecture that combines the strengths of our version of NEMO BS (i.e. UMA) and AAA services in a secure and efficient way and satisfies the requirements of both MNs and ANs.

- Our qualitative evaluation discussed the merits of our approach and how it satisfies the requirements of all the parties involved.

- The results from our thorough quantitative evaluation with different authentication methods and configuration, demonstrated the performance and applicability of our approach for a real world deployment.

Questions?



Thank you!

Panagiotis Georgopoulos (panos@comp.lancs.ac.uk)
http://www.comp.lancs.ac.uk/~georgopp/
Lancaster University

Mobile Router

Vehicle Router