International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Public Network Security and Access Control Based on CoAP

Saiba P. A[1], Aiswarya M. R[2], Anusha Brasha P.P[3], Ashiya Kareem[4], Mufshana M. T[5], Vinduja S. Nair[6]
[1]*Assistant Professor, University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*
[2]*University of Calicut, Computer Science Department, I E S College of Engineering, Chittilappilly, Thrissur, Kerala*

Abstract: ***The internet is the paradigm shift now all over the world, where devices are connected via the same, which help us communicate with each other, gather and share data directly with each other, collect and analyse that data to make our planet intelligent, interconnected and more instrumented. We can't imagine a world without it since it has become an inevitable part in our lives. We prefer a wireless connection over our own data plans since it's free, unlimited and usually faster. But public networks like Wi-Fi comes with lots and lots of issues. Malicious hackers might use Wi-Fi sniffers and other methods to intercept almost all the data that goes through the router. So, its high time we find a very secure and efficient method for authentication and access control for the users who try to access the public networks. This paper proposes a novel technique which implements one of the most promising protocols of IoT called the CoAP into the Wi-Fi routers or access points which enhances the security by providing an encrypted and secure channel for the communicating parties so that no data intrusion or session duplication happens. It is a request-response model. Ticket is used for validation and ECDSA is used to improve the privacy of the system.***

Keywords: ***CoAP, IoT, Ticket, Access Control, Security***

I. INTRODUCTION

There is a lot of hype around the internet now as we all know and it continues to evolve. Many existing mechanisms gives security and protection to networks and systems but they are unable to give fine grain access control. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy and Wi-Fi Protected Access. WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. Also, the risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless access.

Arising access control issues are considered in this work called The Secure and Authenticated CoAP based access control in public networks and IoT. The recent development of IoT or evolution of internet leads to a situation where privacy issue is becoming more and more challenging and personal information such as health-related data, personal and official documents, etc. or other confidential information are kept, monitored and controlled by the network of things. The objective of this CoAP based authentication and access control in public networks or the network of things is to establish a centralized access control system between the connected IoT nodes. Those nodes can be any devices we are working with. They can be PCs or laptops or smartphone, tablets etc. To achieve the proposed objective, a lightweight attribute-based access control system is developed which can verify a request made by a Smartphone or any other powerful devices to READ, WRITE or control other IoT nodes. And the lightweight attribute-based access control system is developed with the help of the Constrained Application Protocol (CoAP).

II. LITERATURE SURVEY

In the work done by Capossele, security is viewed as a CoAP resource. The implementation for IoT is discussed based on the optimized DTLS. We can see that, in spite of the huge diffusion of DTLS, there is a lack of optimized implementations which are introduced to resource constrained devices. Proposes the integrating of the Datagram Transport Layer Security (DTLS) protocol inside the Constrained Application Protocol, exploiting Elliptic Curve Cryptography(ECC) optimizations and minimizing ROM occupancy. This solution suggested by this paper is implemented on an off-the shelf mote platform. The results showed that the

ECC optimizations outperform prior's scalar multiplication in state of the art for class 1 mote platforms. So, ideas came to overcome these demerits [5].

In the work called LESS: Lightweight Establishment of Secure Session proposed by Bhattacharyya, Bose and Pal, a novel technique is introduced for the channel encryption that is established between the communicating parties. The method introduces a cross-layer approach using CoAP and DTLS-PSK. The introduced idea partitions the responsibility of secure communication such that secure session establishment is performed at the application layer and transfer of full application layer message over secure channel is performed by the transport-layer security. The establishment of secure session is implemented as a novel lightweight challenge-response scheme and deployed on CoAP as simply two pairs of encrypted request/responses. This secure session establishment is offloaded to application layer enabling the application layer with greater control while dealing with constrained environments. Also enables CoAP with inherent capability to provide authentication and optional object security to application layer payload.

Skarmeta and Ramos introduced a decentralized approach for security and privacy challenges in the IoT. To overcome the challenges regarding the security and privacy, a capability-based access control mechanism which is built on PKC, and its application in IoT scenarios is introduced. Since typical IoT end devices present severe resource constraints, most of the proposals have addressed this problem by using centralized approaches where a central entity or gateway is responsible for managing the corresponding authorization mechanisms and security protocols. While popular access control models such as RBAC or ABAC and security standard technologies and protocols can be used in these approaches, several drawbacks arise when they are considered in a real IoT deployment [4]. Hence this paper also becomes a victim for replacement.

Pereira, Eliasson and Delsing proposed an authentication and access control framework for CoAP based Internet of Things. In this paper, a CoAP based framework for service-level access control on low-power devices is presented. The framework introduced here allows fine grain access control on a per service and method basis. The aim of the introduced framework was to provide a holistic structure for secure SOA-based low power networks comprise by resource constrain devices. In order to realize the vision of Internet of Things in a secure and efficient manner, the communication between devices must be secured. Even though the use of well-known security mechanisms is vital for SOA-based IoT/CPS networks and systems to be protected, they do not provide any fine grain access control [2].

Finally, Mohsin B Tamboli and Dayanand Ambawade introduced a paper which says the concept of implementing CoAP for a secure and an efficient CoAP based authentication and access control for the Internet of Things [1]. In this paper, we get to see a security model based on challenge-response architecture that uses lightweight protocols to mutually authenticate the CoAP client and server to setup a secure communication channel was discussed in this proposal. The paper discussed the proposed authentication scheme as well as explained the contribution of CoAP which arises as a best alternative to recently used security protocols. This paper gave a total novel idea for introducing this paper on security in public networks using CoAP.

In this paper we propose a security model for accessing public networks like Wi-Fi including all the cool aspects of the above-mentioned papers and overcoming all their demerits. Proposed solution uses Kerberos protocol along with CoAP. ECDSA retains the privacy of communication and gives better security from attacker. The introduced access control layer is beneficial to interrupt any malicious activities too.

III.PROPOSED SYSTEM

This section explains the proposed system along with requirements, access control and authentication.

A. Requirements

The main requirement is to overcome all the faults and follies of the existing public networks by improving the authentication and getting fine grain access control. To improve the security performance, the communication overhead, authentication delay, computational complexity of the system should be very low. The ticket system that is introduced is very unique and efficient enough to distinguish authenticated user from intruder. So only valid devices should be allowed to communicate with the access control services. Advanced encryption schemes must be used to enhance the privacy of communication. Thus, we have used the algorithm ECDSA. Access methods and rules could be changing with authentication policies. Our goal is to present a comprehensive security framework and to give fine grain access control per services.

B. Proposed Architecture

The proposed framework architecture is given in the Figure 1. This describes the system which implements CoAP in the access point. Both the CoAP client and server authenticate each other and if authenticated well, they communicate with appropriate session. The client will be able to access the service from the server. The communication occurs through an encrypted channel.

C. Authentication

It is the procedure to verify that the source is alleged as the messages are not altered. It provides multiple user authentication options including JSP with API. It also supports largest number of users while maintaining smallest amount of code. In this module, the user can be verified related to the existing users or new users. Data can be analysed related to the users' privileges and then the server can be provided and then the data transmission can be accessed related to the users' authentication and access. Checks each users' validity through his ID and password. New user has to make registration on the CoAP server. When user sends request for authentication, its identity is checked against stored data. If matched, then informs the CoAP server. Thus, the user can login successfully.

1) *Trusted List Generation:* Each user list authenticated is recorded and kept in storage for creating list for trusted handshake. The gateway wireless controller does not communicate with APs that are not trusted. If an AP is not trusted, wireless data functions on the AP continue to operate, but the gateway wireless controller does not manage or monitor that AP. APs that are paired with a gateway wireless controller for the first time are automatically trusted. Built-in trusted root certification authority, wireless auto configuration, as well as support for WPA and WEP. For ease of configuration and enhanced security, this paper documents configuration to support client.
2) *Mutual Handshake:* It is a mutual SSL authentication. This is done by the CoAP server. It is based on digital certificate or public key certificate issued by the trusted Certificate Authorities (CA). Certain steps are present in this process. At first, a client requests access to the protected resources. The server then presents its certificate to the client. The client verifies the server's certificate. If successful, the client sends its certificate to the server. The server then verifies the client's credentials. If successful, the server grants the access to the requested resource.

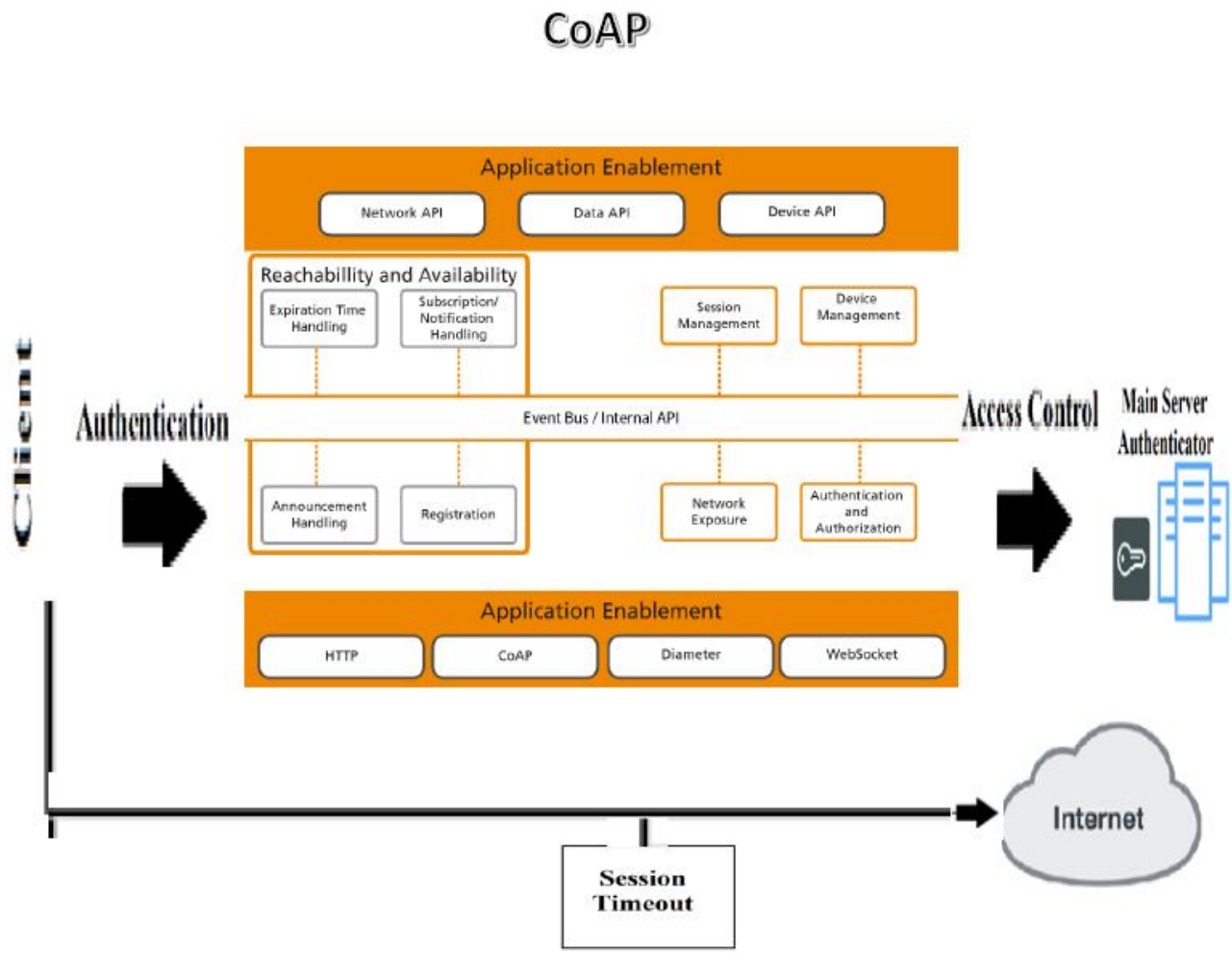

Fig. 1 System Framework

D. Access Control

This is the second process that occurs after the authentication process. It describes how to secure access to network by devices when they initially attempt to access the network. It is done by a middle layer using the CoAP server. The captive portal takes the user to the access control layer. After submitting the OTP, the user can log in. The user gives the access-request to the main server authenticator. The CoAP NAS checks the ticket validity. If the token is valid, access-accept is sent from main server to the CoAP server. On successful verification, the server creates TGS for requested service and can access the required service. A unique encrypted session is then created. If any malicious activity is found, that user is put in blacklist and the session is made to terminate. Using the gateway, the access to data is controlled. The guest permissions are set in the RADIUS server. And the session expires after the timeout. It is done through one-time password, ticket and the main actor, the CoAP server.

1) *CoAP server:* CoAP is one of the most promising protocols for Internet of Things. Its is intended to be used in simple electronic devices and allows them to communicate over the internet. CoAP provides a request/response interaction model between application end-points, supports built-in discovery of services and resources, and includes key concepts of the web such as URIs, RESTful interaction, extensible header options, etc. CoAP easily interfaces with HTTP for integration with the Web while meeting specialized requirements such as multicast support very low overhead and simplicity for constrained environments. CoAP uses UDP unlike HTTP. Some features of CoAP are: -Two types of request messages: confirmable message (CON) and non-confirmable message (NON). The URI format allows the use of standard and specialized service endpoints. CoAP also allows to send very bug messages with a stop-and-wait mechanism called “block wise transfers”. This is where the users register. This is the one who does the access control.
2) *OTP:* The one-time password is sent through the email id or mobile number. OTP is validated and then the user is logged in. RMI is used here to start the services. Kerberos approach provides authentication by generating ticket for valid user. Authentication server must be able to perform login and logout correctly. On successful login, it should generate ticket and logout should delete it.
3) *Ticket:* It is a unique ID generated using Kerberos protocol. It is unique per user and session. It has a particular timeout. The ticket is encrypted using ECDSA algorithm to avoid attack on it. It is generated when the user gives an access request. Only if the ticket is valid, the session is created. TGS and TGT are the two tickets used. TGT is the ticket to get ticket and TGS is the ticket to get the service. The ticket is generated when the user tries to access the web. TGS and the service name is provided to the server to get the service.

IV. IMPLEMENTATION

When a user tries to access a network connection, if he is able to access it so smoothly, then there is great scope for malicious activity to take place. Hence, we have implemented this system. This is implemented to enhance the security of the public networks like Wi-Fi by modifying the CoAP framework.

The user will be asked to sign it to the network. Then a captive portal will be popped in front of the user. Then, he has to enter his registration details like username and password. He also has to type in the OTP that is provided to him via the email id or his mobile number. The details will be checked with that of stored in the CoAP server. If the details and the OTP is true and valid, then the user will be redirected to the service request page he asked for. As the user authenticates and gets logged in after the OTP verification, ticket will be generated which will provide the user access to services on server and it will be unique. The ticket is created when he tries to access the service. Only if the ticket is valid, the service is provided. When successful, a unique session is being created with proper time – out and the communication in that session will be secured and encrypted. The detailed working of the system can be easily understood from the figure 2. This gives the work flow.

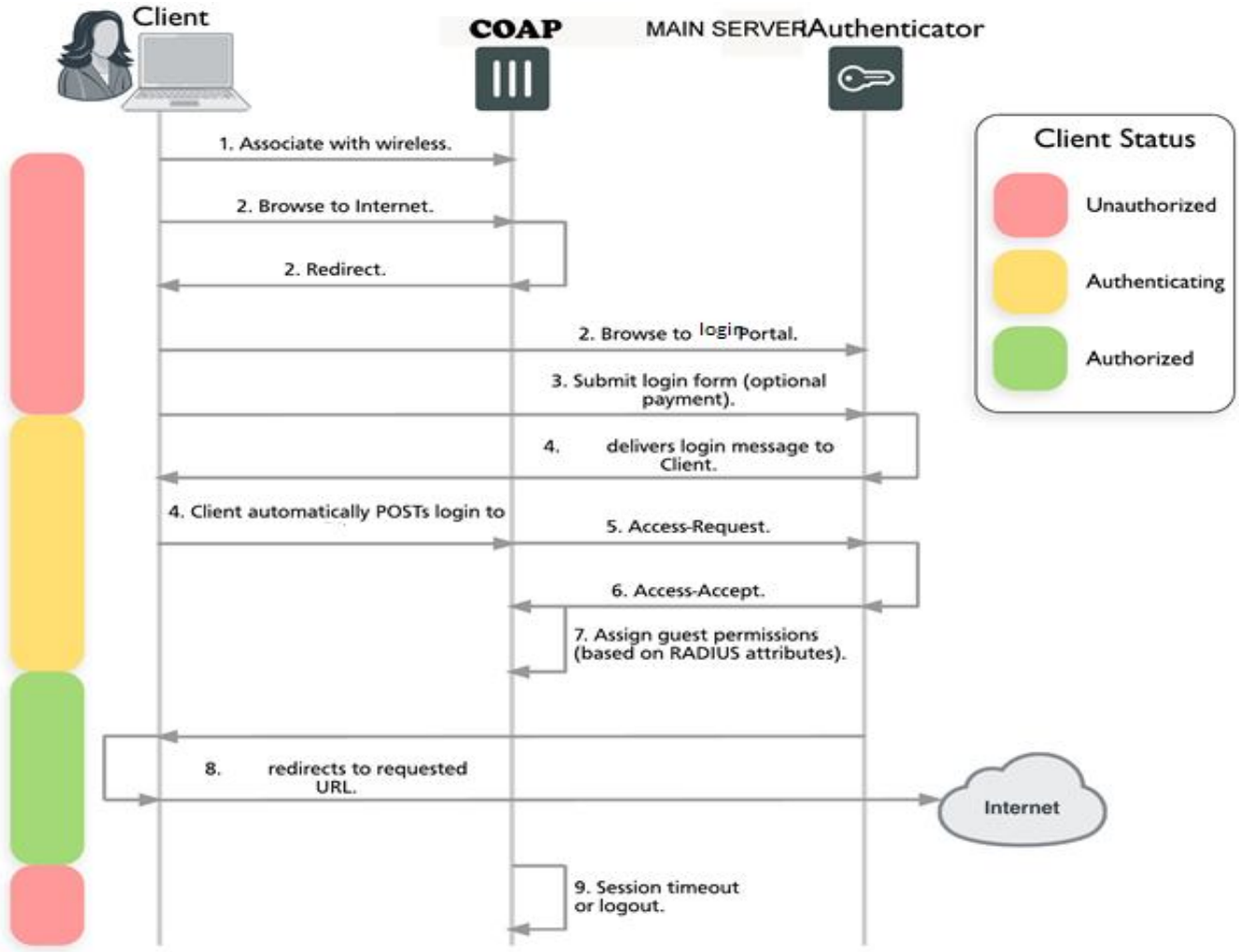

Fig. 1 Work Flow

A client first tries to access internet. Then he is redirected to a captive portal asking the authentication details. The details he entered goes from the CoAP server to the main server authenticator to authenticate. The authentication details are checked with that of the registered details in the CoAP server. The notification indicating successful login or failure will be displayed accordingly. After that the client automatically posts login and an access-request is sent from the CoAP server to the main server authenticator. The unique ticket is generated here based on which an access reject or accept will be replied back from the main server authenticator. According to the positive reply, a unique and encrypted session is created. Guest permissions can be set in the RADIUS server. And he is redirected to the requested URL. Thus, he can access the world wide web until his session timeout. Until submitting the login form, he is in unauthorised stage. From this to setting permission, he is in the authenticating stage. Thus, he gets access to the internet. Now he is in the authorised stage. But he can access the web only until the special session time out. CoAP server can be implemented in any IoT device. We used Raspberry pi here and modified the CoAP framework. The gateway in the CoAP server provides the access control. It interrupts the session if any malicious activity is found. Any data plan, access-list, billing information, usage capacity, graphs, reports of usage can all be manipulated at the server side.

V. CONCLUSIONS

We described through this project, a methodology for the security of public networks using Constrained Application layer protocol(CoAP) and an access control layer. There are no existing systems in which the public networks like Wi-Fi have CoAP implemented in it. The paper discusses the proposed authentication scheme as well as explains the contribution of CoAP. CoAP arises as best alternative to recently used security protocols. Proposed solution uses Kerberos protocol along with it. To access different services on server, special id called ticket is generated. Kerberos, the network authentication protocol is used for the ticket

generation. Ticket is unique per service. ECDSA, the elliptic curve digital signature algorithm reduces the communication overhead and improves the privacy of the communication. Overall authentication delay is reduced in the proposed method since Kerberos reduces the authentication time and ticket granting time. Hence, by overcoming the demerits existing in today's public network, this proposed system can be a good and reliable security solution for public networks and a very beneficial one too.

VI. ACKNOWLEDGMENT

We owe a debt of gratitude to Dr. S. Brilly Sangeetha-Head of Computer Science Department, for the vision and foresight which inspired us to conceive this project. We also show our sincere thanks to Ms. Saiba P.A. who has been guiding us in moulding this project into a successful one.
Above all, we are very much thankful to the Almighty God for showering his blessings upon us for this great success.

REFERENCES

[1] Mohsin B Tamboli and Dambawade, “Secure and Efficient CoAP Based Authentication and Access Control for Internet of Things(IoT)”, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21,2016, India,Pages:1245-1250.
[2] P. P. Pereira, J. Eliasson, J. Delsing, “An Authentication and Access Control Framework for CoAP-based Internet of Things”, Industrial Electronics Society, IECON 2014 – 40th Annual Conference of the IEEE, Year:2014, Pages: 5293-5299.
[3] Antonio F Skarmeta, Jose L. Hernandez-Ramos, M. Victoria Moreno, “Decentralized approach for Security and Privacy challenges in the Internet of Things”, 2014 IEEE International Conference on World Forum on Internet of Things (WF-IoT).
[4] Abhijan Bhattacharyya, Tulika Bose, Soma Bandyopadhyay, Arijit Ukil,and Arpan Pal, “LESS:Lightweight Establishment of Secure Session”, 2015 29th International Conference on Advanced Information Networking and Applications Workshops of the IEEE.
[5] Angelo Capossele, Valerio Cervo, Gianluca De Cicco and Chiara Petrioli, “Security as a CoAP Resource: an optimized DTLS implementation for the IoT”, IEEE ICC 2015 SAC on Internet of Things
[6] Xi Chen, “Constrained Application Protocol for Internet of Things”, April 2014, http:/www.cse.wustl.edu/jain/cse57414/ftp/coap/i ndex.html.
[7] E. Poenaru, C. Poenaru, “A Structured Approach of the Internet-eHealthUseCases,”4thIEEEconferenceonEHealthandBioengineering Year:2013
[8] Balandina E., Balandina S., Koucheryavy Y., Mouromtsev D., “IoT Use Cases in Healthcare and Tourism,” IEEE 17th Conference on Business Informatics, Year:2015
[9] Angelo P. Castellani, MattiaGheda, Nicola Bui, Michele Rossi, Michele Zorzi, “Web Services for the Internet of Things through CoAPand EXI,” IEEE International Conference on Communications Workshops (ICC),5- 9 June 2011, pp. 1-6