JSCSE

Table of content
Vol. 2, No. 7, July 25, 2012

Abstract . Software development projects are subject to risks like any other project. These risks must be managed in order for the project to succeed. Current frameworks and models for risk identification, assessment and management are static and unchanging. They lack feedback capability and cannot adapt to future changes in risk events The OODA (Observe, Orient, Decide, Act) Loop, developed during the Korean War by fighter pilot Colonel John Boyd, is a dynamic risk management framework that has built in feedback methods and readily adapts to future changes. It can be successfully employed by development teams as an effective risk management framework, helping projects come in on time and on budget.

Keyword : OODA Loop, risk management, software development

Abstract . A Mobile Ad Hoc Network (MANET) comprises mobile nodes, equipped with wireless communications devices; which form a temporary communication network without fixed network infrastructure or topology. The characteristics of MANET are: limited bandwidth; limited radio range; high mobility; and vulnerability to attacks that degrade the signal to noise ratio and bit error rates. These characteristics create challenges to MANET routing protocols. In addition, the mobility pattern of the mobile nodes (MNs) also has significant impact on the MANET routing protocols. The issue of routing and maintaining packets between MNs in the mobile ad hoc networks (MANETs) has always been a challenge; i.e. encountering broadcast storm under high node density, geographically constrained broadcasting of a service discovery message and local maximum problem under low node density. This requires an efficient design and development of a Lightweight routing algorithm which can be handled by those GPS equipped devices. Most proposed location based routing protocols however, rely on a single route for each data transmission. They also use a location based system to find the destination address of MNs which over time, will not be accurate and may result in routing loop or routing failure. Our proposed lightweight protocol, Local Area Network Dynamic routing (LANDY) uses a localized routing technique which combines an unique locomotion prediction method and velocity information of MNs to route packets. The protocol is capable of optimising routing performance in advanced mobility scenarios, by reducing the control overhead and improving the data packet delivery. In addition, the approach of using locomotion prediction has the advantage of fast and accurate routing over other position based routing algorithms in mobile scenarios. Recovery with LANDY is much faster than with other location protocols which use mainly greedy algorithms, (such as GPRS), no signaling or configuration of

the intermediate nodes is required after a failure. The key difference is that it allows sharing of locomotion and velocity information among the nodes through locomotion table. Simulation results show that LANDY`s performance improves upon other position based routing protocols.

Keyword : Ad hoc network, light-weight , Hybrid network, Wireless Network, Mobility predication.

Design of an Encryption-Decryption Module Oriented for Internet Information Security SOC Design

Yixin Liu, Haipeng Zhang, Tao Feng

Doi : 10.7321/jscse.v2.n7.3

Abstract . In order to protect the security of network data, a high speed chip module for encrypting and decrypting of network data packet is designed. The chip module is oriented for internet information security SOC (System on Chip) design. During the design process, AES (Advanced Encryption Standard) and 3DES (Data Encryption Standard) encryption algorithm are adopted to protect the security of network data. The following points are focused: (1) The SOC (System on Chip) design methodology based on IP (Intellectual Property) core is used. AES (Advanced Encryption Standard) and 3DES (Data Encryption Standard) IP (Intellectual Property) cores are embedded in the chip module, peripheral control sub-modules are designed to control the encryption-decryption module, which is capable of shortening the design period of the chip module. (2) The implementation of encryption-decryption with hardware was presented, which improves the safety of data through the encryption-decryption chip and reduce the load of CPU. (3) In our hardware solution, two AES (Advanced Encryption Standard) cores are used to work in parallel, which improves the speed of the encryption module. Moreover, the key length of AES (Advanced Encryption Standard) encryption algorithm is designed with three optional configurations at 128 bits, 256 bits and 192 bits respectively and six optional encryption algorithm modes: CBC (Cipher Block Chaining) mode, ECB (Electronic Code Book) mode, GCM (Galois/Counter Mode) mode, XTS(cipherteXT Stealing) mode, CTR (CounTeR) mode and 3DES respectively, which adds the flexibility to its applications.

Keyword : encryption-decryption module, IP core, SOC, 3DES, AES

Research on the Algorithm of the Trustful Communication over the Metrized Small World Distributed Data Storage System

Dmitry Gusev

Doi : 10.7321/jscse.v2.n7.4

Abstract . In ideal distributed network each node is in trust with all others. But in a real world there is no guarantee that all the nodes will operate with their prescribed rules. There might be ones which malfunction because of the incorrect internal object state and the ones which are infected by an external subject. These use cases reveal the need in trust policies utilized in the network. Because of the distributed nature of the system more effective security algorithm will be the one which implies the trust evaluation without centralized authorities. In this paper we investigate a possibility of developing the secure network where its actors can fully trust each other over the

system Metrized Small World (MSW) from the Meralabs LLC.
Keyword : distributed data storage, Metrized Small World, semi-metric, trust propagation, trust model, trustful search algorithm

CLTChord: Improving lookup at the Chord protocol using cache location table
45-54

Jaber Karimpour, Majid Moghaddam, Ali A. Noroozi

Doi : 10.7321/jscse.v2.n7.5

Abstract . Peer-to-peer networks have emerged as a common method for sharing large amounts of data. The main challenge in these networks is efficiently locating information distributed across the hosts/peers of the network by decentralized approach. In this paper, first we refer to the Chord protocol that is a distributed lookup service, and then propose a new method, called CLTChord, to optimize this protocol. In this new method, in addition to using the local finger tables for routing requests, the cache location tables are used, in which each node stores nodes which are at its close geographical range. When a node receives a new request, it first checks its cache location table and if a desired response is not received, the algorithm continues to work like the basic Chord protocol. Our simulation shows that this optimization improves the parameters of the hop count, the lookup latencies and number of the sent packets; In this paper, hop count is the distance between the source node which initiates the lookup and the target node which has the desired value; and latency is the duration of time needed for resolving file lookups from the time when it was initiated until it was responded to (measured in milliseconds).
Keyword : Communication networks, Peer-to-peer, Chord, Finger table

A Prediction Model for System Testing Defects using Regression Analysis
55-68

Muhammad Dhiauddin Mohamed Suffian, Suhaimi Ibrahim

Doi : 10.7321/jscse.v2.n7.6

Abstract . This research describes the initial effort of building a prediction model for defects in system testing carried out by an independent testing team. The motivation to have such defect prediction model is to serve as early quality indicator of the software entering system testing and assist the testing team to manage and control test execution activities. Metrics collected from prior phases to system testing are identified and analyzed to determine the potential predictors for building the model. The selected metrics are then put into regression analysis to generate several mathematical equations. Mathematical equation that has p-value of less than 0.05 with R-squared and R-squared (adjusted) more than 90% is selected as the desired prediction model for system testing defects. This model is verified using new projects to confirm that it is fit for actual implementation.
Keyword : prediction model, system testing, regression analysis, defects, defect prediction

CBM-Of-TRaCE: An Ontology-Driven Framework for the Improvement of Business Service Traceability, Consistency Management and Reusability
69-78

Aida Erfanian, Nima Karimpour Darav

Doi : 10.7321/jscse.v2.n7.7

Abstract . In this paper, we represent a CBM-Of-TRaCE which is an ontological framework that integrates two aspects of business components: conceptual and methodology. In the development of our framework we have taken IBM's Actionable Business Approach (ABA) in to consideration. We evaluate our framework through some aspects such as support and facilitation for a business from five different aspects: service-orientation, business process, management integration, reusability improvement, consistency rules, and traceability. As well, we demonstrate the compatibility of our CBM-Of-TRaCE with ABA's four phases.

Keyword : Component Business Model (CBM), Service Oriented Architecture (SOA), Business Service, Traceability, Reusability, Actionable Business Approach (ABA), Ontology

Free Access and
More Information

For This Volume

JSCSE

Editorial Board
Vol. 2, No. 7, July 25, 2012

V

JSCSE