DOI 10.12694/scpe.v20i1.1519
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 20, Number 1, pp. iii–iv. http://www.scpe.org

INTRODUCTION TO THE SPECIAL ISSUE ON OPPORTUNISTIC NETWORK AND ITS SECURITY CHALLENGES

It is our great privilege to present before you Volume 20, Issue 1 of the Scalable Computing: Practice and Experience. We had received 41 paper submissions from Belgium, Malaysia, Indonesia, Bangladesh, Yemen and India, and selected 12 papers for publication. The acceptance rate of this issue is 29 percent. The aim of this special issue is to give the solutions of opportunistic networks and security challenges as well as to collect other research problems in opportunistic networks for further research. This special issue gives the new dimensions for opportunistic networks in the perspective of research.

Ritu Nigam et al. had tried to investigate the contact information and social pattern of the node and propose a message forwarding technique in the social opportunistic network. To obtain the contact information and social pattern of nodes, a bonding metric is constructed to show the direct and indirect bonding of neighboring nodes in the system. As the detachment period contains both the encountered frequency and duration of their connections in the vicinity of its neighbors, it is precise to use it to illustrate the direct bonding in the neighboring relationship. It also incorporates the indirect bonding of nodes by identifying weakest direct bonded nodes to replace it with active indirect bonded nodes of the network. The results depict that the proposed protocol can significantly raise the forwarding efficiency concerning the number of messages delivered, overhead ratio, message dropping, and average latency.

Md. Sharif Hossen et al. presented the paper on Analysis of delay tolerant networks routing protocols using the impact of mobility models. In an intermittently connected mobile network, the communication among the mobile nodes can be established easily using the store-and-forward strategy. This network is also called delay-tolerant which can allow the long latency, irregular data rates, and disruption in mobility. Under such a network scenario, the authors had analysed the impact of mobility models using the performance of several delay-tolerant routing protocols. Hence, they simulate the scenario using the opportunistic network environment simulator. Considering three performance metrics namely, deliver probability, latency, and overhead ratio it was seen that spray-and-focus showed good performance while epidemic gave poor results among the routing techniques considered. Furthermore, shortest path map based movement mobility model deserves good performance compared to random walk and random direction.

Deepak Kumar Sharma et al. presented the paper on Establishing Reliability for Efficient Routing in Opportunistic Networks. The Reliability in Oppnet (RIO) protocol is a reliable protocol that improves the routing in Oppnet and works in combination with the existing routing protocols. RIO makes the source node aware about the status of the message so that if an error occurred in routing then the source node can take suitable action like resending of the message and error reporting. In this work, solutions are provided for five errors namely redirection error, buffer overflow error, parameter problem, Time Limit Exceeded i.e. TTL expiration error and destination unreachable. Through simulation using ONE simulator it has been found that RIO enhances the Spray and Wait routing protocol while working in parallel with it.

Pawan Singh Mehra et al. propound E-CAFL which is an enhancement over CAFL protocol. It takes remnant energy, node density and distance from the sink as input to Fuzzy Inference System for calculating the rank of each sensor node for cluster head candidature. Also, member nodes intelligently select their cluster head on the basis of Cluster Head-Chance which takes into account the rank of the cluster head and distance to that cluster head nodes during cluster formation. Simulation experiments have been performed for the designed protocol. It has been observed from the results that E-CAFL has better stability period and protracted lifetime as compared to LEACH and CAFL protocol.

Rajan Sharma et al. proposed Zone-based Energy Efficient Routing Protocols for Wireless Sensor Networks, is a zone-based framework that focused on minimizing the energy consumption in the re-selection process of zone-head (ZH). In this novel ZH re-selection process, the number of control messages exchanged during the selection process of ZH significantly reduces and it helps to achieve a prolonged lifetime. In addition to that the stability version of the above-said algorithm is proposed, that improves the stability period of the network by selecting ZH on the basis of residual energy.

Arvinda Kushwaha et al. presented an overview of the integration of the wireless sensor network and cloud computing. Particle swarm optimization (PSO) is used to optimize resources. The optimization is done through the load scheduling algorithm. This paper proposed load scheduling algorithm that is based on the particle

swarm optimization technique which is used to optimize total transfer time and cost. Simulation result shows that the proposed method is better than the conventional method.

Musaeed Abouaroek et al. proposed the NTRU algorithm for node authentication in opportunistic networks. NTRU algorithm comes in the category of post-quantum cryptography. It is unbreakable and fast than the RSA algorithm and Elliptic Curve Cryptography.

Suman Bala et al. presented the paper on the security of authenticated group key agreement protocols. The authors analyzed the two AGKA protocols against attacks and found both protocols are insecure. In addition, they fixed the vulnerabilities of Tans protocol.

Pankhuri Sai et al. proposed a user authentication scheme which is one of the most important components of a secure system. Even after the development of advanced authentication mechanisms such as biometrics, the traditional concept of passwords still continues to be the most widely adopted means for user authentication. Owing to the limitations of text-based passwords such as smaller password space, susceptibility to brute force attacks; and that of graphical passwords like shoulder surfing attacks, this paper proposed a novel pattern-based multi-factor authentication scheme that involves the use of a combination of textual and graphical passwords. The proposed system has a larger password space and is secure against shoulder surfing and dictionary attacks since it involves additional mouse input along with the keyboard input. Moreover, a brute force attack is also infeasible for it.

Asif Iqbal Hajamydeen et al. presented about the Intrusion detection systems (IDSs) in the paper. The growing number of the Internet users has paved the way in improving the Internet availability infrastructure to make the facilities accessible through various devices but failed to address the arising security issues. The ubiquitous nature of todays Internet agrees with devices or applications that have adapted the technology to link with the Internet which has brought the challenge in providing network security. In the current scenario with interactions between untrusted clients and networks, the network infrastructures are very defenceless. To defend such situations efficiently, intrusion detection systems (IDSs) were used to deliver a self-defensive power for a system or a network. Therefore, this paper provides an overview and review of data mining-based intrusion detection approaches and also those utilizing heterogeneous logs for intrusion detection. Conclusively, it proposes the characteristics to be contained in future intrusion detection model/framework, ways by which the classification/clustering algorithms to be utilized in the model and the considerations on choosing the data to be tested, in order to detect intrusions effectively.

Chanchal Kumar et al. presented the need for designing a security system for a network system arises due to the greater complex structure. An extended protocol for hiding pertinent information based on a fast Diffie-Hellman using Kummer Surface is described in the paper. The extended protocol is devised by the inclusion of an additional point in the Kummer surface for higher security need. Further, the use of a machine learning method is illustrated, which is employed for the selection of a specific surface from a set of available Kummer surfaces. The use of NSGA-2 algorithm is next described for selection of a specific surface. The newer version of key expansion of the AES-128 algorithm is described and illustrated in the paper. This version is based on a newly devised content-matrix. The scheme adopted for the construction of content-matrix is fully illustrated and an optimization algorithm used in the scheme is given along with the outputs obtained with sample data. The outputs of the new version of key expansion are given. The LIM index that is commonly used for cryptanalysis purpose is described next. Hence, the cryptosystem based on extended Kummer surface and new scheme adopted for key expansion of AES-128 could provide useful techniques for hiding the information in a network system. The use of machine learning and NSGA-2 algorithm could enhance automatic selection for a specified extended Kummer surface. These tools can be quite useful for a cryptosystem designer.

Hamza Mutaher et al. proposed the Zero-Knowledge Proof Based Identification Scheme for Securing Software Defined Network. Due to the leak of security in SDN network, many types of attack like host impersonation attack, Man-in-the-middle attack and Denial of service attack can penetrate into the controller to control the whole network or to shut the network totally down. In this paper, a Zero-knowledge proof based identification scheme has been proposed to secure the SDN controller while the data and control planes establish communication. In this security scheme, the user does not need to send his password to the controller in every login attempt. Instead, the authentication server will share the same secret between both user and controller; the user has to prove to the controller that he knows the secret without revealing the exact secret. Communication

and competition costs along with storage overhead analysis are discussed as well in order to validate this work.

We would like to express our sincere thanks go to the chief editor, editorial board members and reviewers who have reviewed the manuscripts within the time to publish this special issue on the scheduled date.

Rosilah Hassan, Universiti Kebangsaan Malaysia, Malaysia
Khairol Amali Bin Ahmad, National Defence University of Malaysia, Malaysia
Khaleel Ahmad, Maulana Azad National Urdu University, India