



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Trust Oriented Secure Ad hoc Networks: A Generic Framework

Amandeep Verma¹ and Manpreet Singh Gujral²

¹Punjabi University Regional Centre, Mohali

²University College of Engineering, Punjabi University Patiala

Abstract: Due to nonexistence of or little of pre-existing communication infrastructure, ad hoc network permits wireless mobile nodes to self-organize into random and momentary network topologies. Security is a critical concern in ad hoc networks owing to its intrinsic vulnerabilities. A number of security solutions are suggested in the literature but still more is needed. Augmentation of trust to the existing security infrastructures would enhance, on the whole, security of these environments, but most of the studies in literature include trust modeling in the protocol. By this means trust is a foreign component i.e. not a part of the structure itself. Thus its effectiveness is restraint to that protocol. So a framework is desirable with trust as an integral component. The paper presents a desirable framework. At present, Trust modelling is mostly hard-coded into an application, which augments its complexity as well the incapacity to adapt to changes. This can also restrict the usage of those trust models for other protocols and for different network activities. The present study introduces an independent trust model for ad hoc networks. It provides the separation between application and trust model. A functional scenario depicting the usage of said model in ad hoc network environment is also presented.

Keywords: Ad hoc network, framework, trust model

I. Introduction

Ad hoc networks are illustrated by infrastructure less, multi-hop wireless connectivity and recurrently changing network topology. This is primarily owing to decentralization of control and indeterminate users, in open environments. The ad hoc networks are not an alternative or substitution of the networks with infrastructures. Their extent is in the locale where it is likely unrealistic or infeasible to deploy infrastructure

Security is a critical concern in ad hoc networks owing to its intrinsic vulnerabilities. These vulnerabilities are nature of its structure that cannot be eliminated. Consequently, attacks with malicious objectives have been and will be devised to make use of these vulnerabilities and to perturb its operations

A number of solutions are proposed which lessen the vulnerability of ad hoc networks to some extent [10][13][15][27]. One single security solution is not enough to guard against a range of attacks on mobile ad hoc network. Therefore, there is need to apply a multi-defense security solution that offers multiple lines of defense against many different attacks. It is concluded from the literature that usage of trust as supplementary security measure for various network activities of ad hoc network has been proved to very effective. So, trust can be supplemented as additional security measure to offer multiple defense security solution.

Most of the studies reviewed in literature [1][2][4] use trust as a foreign component to ad hoc network environment, with an intention to improve security in such types of network [2][4][11][14]. Accordingly it is concluded that a comprehensive and appropriate framework with trust as integral component is missing, so there is a need of framework that will provide the researchers with a template where they endow with their own method for trust evaluation, updation and even propagation, with same environment for the rest of the network. A trust oriented framework is proposed in section III of this paper.

Trust modelling is mostly hard-coded into an application [1][7][17], which augments to the complexity of the application. Moreover, this approach can raise the issues like inflexibility, dependency, and non-scalability. A separation of the application's purpose and its trust management framework i.e. trust model, will offer a more scalable and flexible solution [8]. An independent trust model is intended to carry out the trust appliance, trust assessment and trust configuration irrespective of its applicability to network activities (routing, authentication or access control) and the protocol used for that activity.

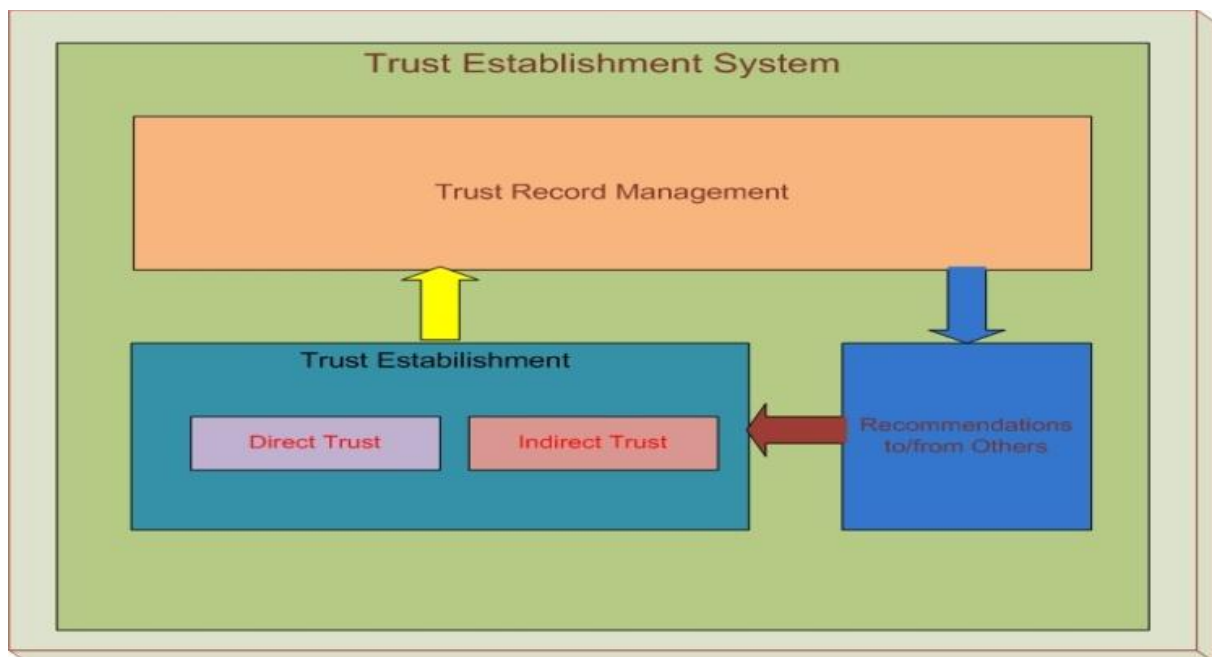
This paper introduces the basic trust oriented security framework for ad hoc networks and the associated trust model. The paper is intended for the researchers having interest in trust oriented framework for ad hoc networks as well the trust model. The paper is organized as follows. The section 2 presents the review of literature. The section 3 gives overview of basic framework and Section 4 presents the proposed trust model with its components and section 5 concludes the paper.

II. Review of Literature

Trust has its appliance in diverse disciplines of the computing. It ranges from social networks [9], E-Commerce [19], Grid [21] and distributed networks [12]. The effect of trust inclusion in ad hoc network has positive impacts. A number of studies support this viewpoint. A trust evaluation based security solution in ad hoc network [28] where Trust is based on experience statistics, intrusion detection results, and reference by other node, owner's preference and policy. In Trust based Adaptive on Demand Adhoc Routing Protocol [17], trust is based upon a node has on its neighbor, different trust level defined and security is applied accordingly. Highly secure, save node's power and even the time for communication is less. A trusted routing solution [23] in mobile ad hoc networks presents a model for computing, distributing and updating trust and proved very good against colluding malicious nodes.

A trust based framework [5] should considers a fully distributed decision process, irrespective to variation in membership, no interference to the device computation and communication resources, no assumption about the cooperation among nodes and self-organized reconfigurable manner so as not to be disrupted by the dynamics of the environments. The basic elements of trust establishment system are as shown in Figure 1.

Figure 1: Basic Elements in Trust Establishment System

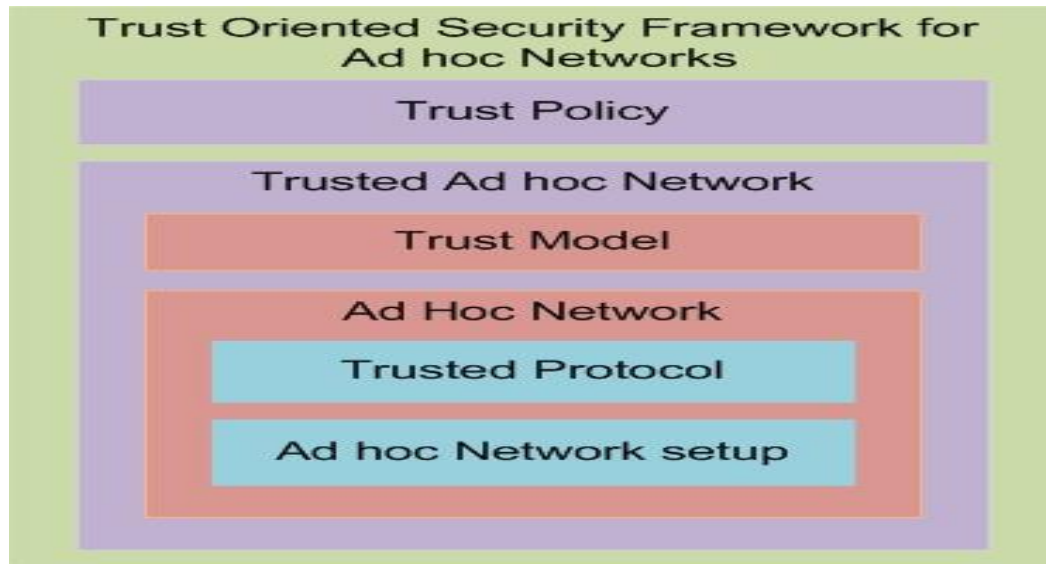


III. A Framework

A framework can act like map that give coherence to empirical inquiry. For software development point of view, a framework, that is used by software developers to implement the standard structure for an application. A basic trust oriented security framework for ad hoc networks is shown in Figure 2.

The ad hoc network setup involves the ad hoc network environment and the trusted protocol is the modified version of the protocol of network activity adapted to make decisions on the basis of trust. The trust model as proposed in the next section is intended to provide the trust modeling to ad hoc network. The trust model and the ad hoc network form the trusted version of the ad hoc network. This version with the trust policy, governs the network, resulted a trust oriented framework for ad hoc network.

Figure 2: Trust Oriented Framework for Ad hoc Networks



IV. Basic Trust Model

The trust model is intended to work as a trust service [18][20][24]. This service is accountable for the trust evaluation, trust updation and trust propagation. This trust service is called for in the situation where the recommendation from the rest of the nodes in the network is required by a node in the network. A basic trust model is developed and is shown in the Figure 3. The various components of the model are as follows

1) Node(s)

These are the active nodes of an ad hoc network. Each of the node has some role in the process of trust evaluation. It may be source node, target node or role as direct neighbor, neighbor of neighbor and others i.e. not falling in other category as listed above.

2) Trust

Trust is the extent to which one party is willing to participate in a given action with a given partner. It is usually a combination of direct and indirect trust or recommended trust. The direct trust is the value of trust a source node has on target node as per their records. The indirect trust is the value of trust a source node has on target node as per the recommendations provided by the rest of the nodes in the network.

Weighting Factors

These are the weighting factor given to trust observations in order to control its impact on the overall evaluation of the trust. As the final trust evaluation has two components- direct and indirect trust. So the sum of the weight of the direct trust and weight of indirect trust is required to be 1.0. Similarly the recommended trust is combination of recommendations from neighbors, neighbors of neighbors and other, so the sum of weights of all recommendation is need to be 1.0.

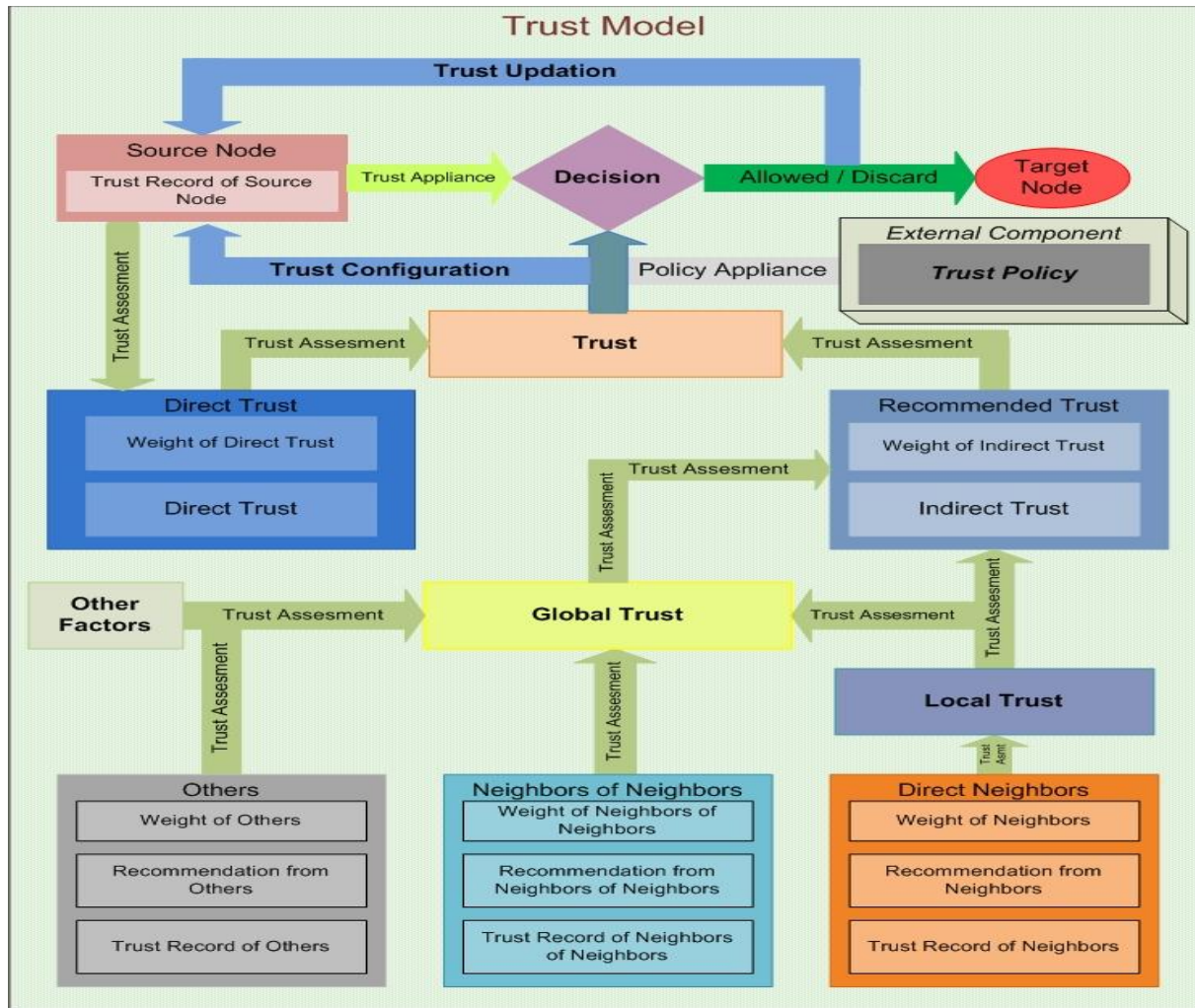
Trust Records

This is the information that is kept by every node about the trust values on other nodes. This information can be a part of information repositories of a protocol.

3) Other Terms

There are factors that can be used to control the trust evaluation process or to put more constraints on the evaluation process of trust assessment for indirect trust. Global Trust is type of indirect trust when the source node wants the recommended trust from all nodes i.e. direct neighbors, neighbors of neighbors and others as defined above, in the network. Local Trust expects only the recommended trust from direct neighbors of the source node. There are some other factors like familiarity of sender node with recommender nodes on the basis of its earlier experiences with them or the similarity in trust recommendations by recommenders.

Figure 3 : Trust Model



Behaviour of the Trust Model

On receiving the request from source node about the trust appliance to make decision regarding whether to allow or discard the interaction with target node, trust assessment begins. The final trust is a combination of direct and indirect trust. The direct trust gets observed from the trust record of the source node. Depending on the type of indirect trust- Global or Local trust, recommended trust from rest of the nodes observed. All these recommendations are combined as per the weighting factor corresponding to the type of recommendations. Finally direct and indirect trust is combined with corresponding weight factors to get the final value of trust assessment. This value is used to configure the new trust value for target node in the information repository of source node. As per the constraints specified in the policy which is an external component i.e. not a part of this model, on the final value of trust assessment, the decision regarding whether to allow or discard the interaction, updates the trust value of target node by source node accordingly.

4) Characteristics of Model

The following are the characteristics assumed by the proposed model.

- **Dynamicity:** The trust is dynamic in nature, as the value of trust gets updated after every interaction.
- **Subjectivity:** The trust depends on the target node and the proximity of the recommenders to the source node, so trust is subjective in nature.
- **Scalability:** The component of trust model "Other Factors" allow the provision to allow more factors in the process of trust assessment.
- **Distributed:** The trust assessment is distributed, as it involves majority of the nodes of the network at that instance.

- Flexibility: The model is flexible but with some limitations e.g. additional class of recommenders can be added or existing class of recommenders can be removed.

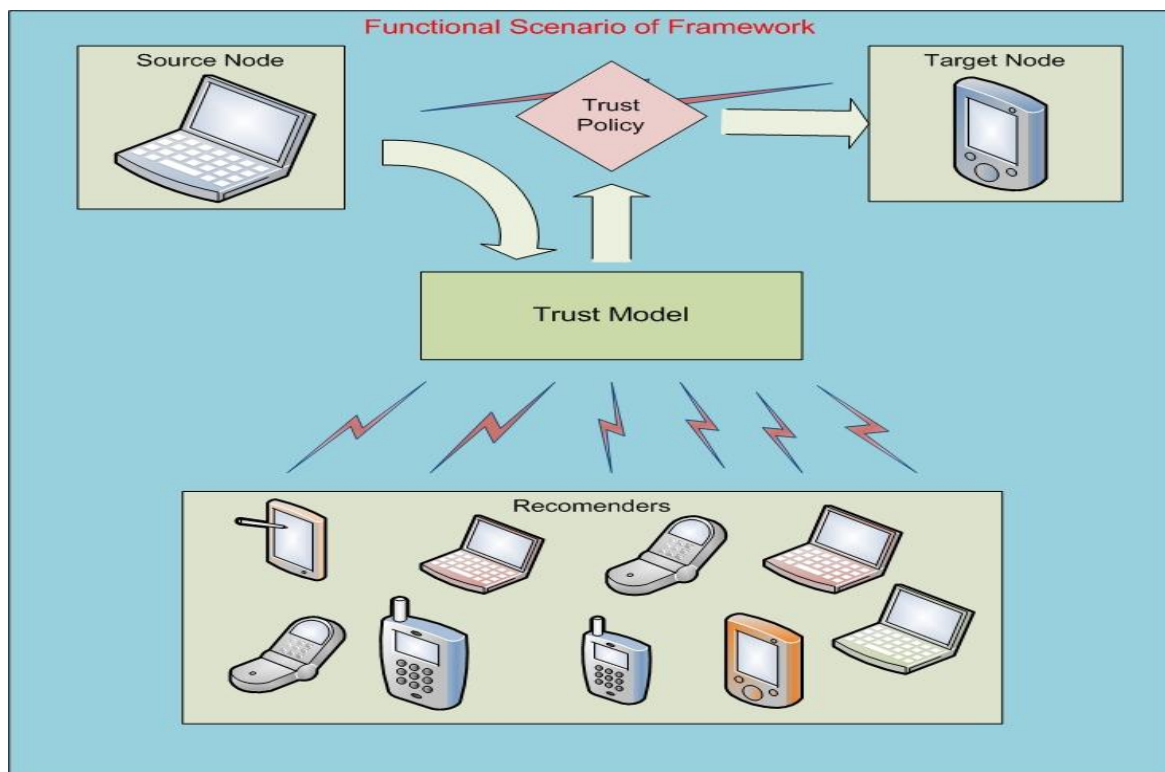
5) Assumptions of Model

The suggested model has one component that serve as the information repository of the node provided by the protocol or by the node to keep the trust values. Moreover the model assumes that the protocols are able make decisions on the basis of trust value(s). So the requirement is that the protocols of the ad hoc networks have functionality to make decisions on the basis of trust and have some means to keep the trust values in its information repositories.

V. Conclusion

A functional scenario of the framework is shown in Figure 4. The scenario depicts the interactions among various components of the ad hoc network. As shown the trust model is an integral component of the environment but as an independent module from the rest of the network environment.

Figure 4: Functional Scenario of Framework



References

- [1] Bhalaji N., Sivaramkrishnan A. R., Banerjee S., Sundar V. and Shanmugam A., "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", *World Academy of Science, Engineering and Technology*, pp. 1074-1079, 2009
- [2] Boukerch A., Xu L. and Khatib K. EL, "Trust-based security for wireless ad hoc and sensor networks", *Computer Communications*, vol. 30, issue 11-12, pp. 2413-2427, 2007
- [3] Brewster C. and O'Hara K., "Knowledge representation with ontologies: present and future", *IEEE Intelligent Systems*, vol. 19, issue 1, 2004.
- [4] Chatterjee Pushpita, "Trust Based Clustering and Secure Routing Scheme for Mobile Adhoc Networks", *International Journal of Computer Networks & Communications*, vol. 1, no. 2, pp. 84-97, 2009
- [5] Cho Jin-Hee, Swami Ananthram and Chen Ing-Ray, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562-583, 2011
- [6] Dayong Ye, Quan Bai and Minjie Zhang, "Ontology-Based Knowledge Representation for a P2P Multi-agent Distributed Intrusion Detection Systems," in *Proc. of International Conference on Network and Parallel Computing*, pp. 111-118, Oct. 2008

- [7] Edith C.H. Ngai and Michael R. Lyu, "An Authentication Service Based on Trust and Clustering in Wireless Ad Hoc Networks: Description and Security Evaluation," in *Proc. of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, pp.94-103, 2006
- [8] Grandison Tyrone and Sloman Morris, "A Survey of Trust in Internet Applications," *IEEE Communications Surveys and Tutorials*, vol. 3, issue 4, pp. 2-16, 2000
- [9] Guanfeng Liu, Yan Wang and Mehmet Orgun, "Trust Inference in Complex Trust-Oriented Social Networks," in *Proc. of International Conference on Computational Science and Engineering*, vol. 4, pp.996-1001, 2009
- [10] Li Wenjia and Joshi Anupam , "Security Issues in Mobile Ad hoc networks -A Survey," *The 17th White House Papers Graduate Research In Informatics at Sussex*, pp.1-23, 2004.
- [11] Li Xiaoqi, Lyu, M.R. and Liu Jiangchuan, " A Trust Model Based Routing Protocol for Secure Ad Hoc Networks", in *Proc. of IEEE Aerospace Conference*, vol. 2, pp. 1286-1295, 2004
- [12] Liang Ge, Jimzhou Luo and Yaobin Xu , "Developing and Managing Trust in Peer-to-Peer Systems", in *Proc. of International Conference on Database and Expert Systems Applications*, pp. 687-691, 2006.
- [13] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks," *IEEE Networks Magazine*, vol. 13, pp. 24-30, 1999
- [14] Martucci L.A., Schweitzer C.M., Venturini Y.R., Carvalho T.C.M.B. and Ruggiero W.V., "A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks", in *Proc. of the 3rd Annual Mediterranean Ad Hoc Networking Workshop*, pp. 278-290, 2004
- [15] Michele Nogueira Lima, Aldri Luiz dos Santos and Guy Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 66-77, 2009
- [16] Mohsen Taherian, Rasool Jalili, Morteza Amini, "PTO: A Trust Ontology for Pervasive Environments", in *Proc. of IEEE International Conference on Advanced Information Networking and Applications*, pp. 301-306, (2008).
- [17] Nekkanti Rajiv K. and Lee Chung-wei, "Trust Based Adaptive on Demand Ad Hoc Routing Protocol", in *Proc. of the ACM Southeast Regional Conference*, pp. 88-93, 2004
- [18] Park Seong-Soo, Lee Jong-Hyouk and Chung Tai-Myoung, "Cluster-Based Trust Model against Attacks in Ad-Hoc Networks", in *Proc. of Third International Conference on Convergence and Hybrid Information Technology*, vol. 1, pp.526-532, 2008
- [19] Qin Zheng and Tian Bo, "A Trust Evaluation Model for B2C E-commerce", in *Proc. of IEEE International Conference on Service Operations and Logistics, and Informatics*, pp. 1-6, 2007
- [20] Rahman Alfarez Abdul and Hailes Stephen, "A Distributed Trust Model", in *Proc. of the ACM workshop on New security paradigms*, pp. 48-60, 1998
- [21] Shaomin Zhang, Yue Zou and Baoyi Wang, "A Novel Grid Trust Model based on Fuzzy Theory", in *Proc. of International Conference on Network and System Security*, pp. 203-207, 2009
- [22] Stefania Galizia, Alessio Gugliotta and John Domingue, "A Trust Based Methodology for Web Service Selection", in *Proc. of IEEE International conference on Semantic Computing*, pp. 193-200, 2007
- [23] Tirthankar Ghosh, Niki Pissinou and Kami Sam Makki, "Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks", *International Journal of Mobile Networks and Applications*, pp. 985-995, 2005
- [24] Velloso P.B., Laufer R.P., Duarte O. and Pujolle G, "Analyzing a Human-based Trust Model for Mobile Ad Hoc Networks", *IEEE Symposium on Computers and Communications*, pp. 240-245, 2008
- [25] Wang Hua, "Research on the model of knowledge representation ontology based on framework in intelligent learning system", in *Proc. of International Conference on Electrical and Control Engineering*, pp. 6757-6760, 2011
- [26] Wanita Sherchan, Surya Nepal, Jonathon Hunklinger, Athman Bouguettaya, "A Trust Ontology for Semantic Services", in *Proc. of IEEE International Conference on Services Computing*, pp. 313-320, 2010
- [27] Yang Hao, Luo Haiyun, Ye Fan, Lu Songwo and Zhang Lixio, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Communications*, vol. 11, issue 1, pp. 38-47, Feb 2004
- [28] Z. Yan, P. Zhang and T. Virtanen, "Trust Evaluation Based Security Solution in Ad hoc Networks", *Technical Report, Nokia Research Center*, 2003