Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 3, No.7, 2012

An Improvement to Trust Based Cross-Layer Security Protocol against Sybil Attacks (DAS)

R. Naveen Kumar[1*] V. Bapuji[1] Dr. A. Govardhan[2] Prof. S.S.V.N. Sarma[3]

1. Department of Informatics, Kakatiya University, Warangal, India
2. Department of CSE, Jawaharlal Technological University (JNTUH), Hyderabad, India
3. Department of CSE, Vaagdevi College of Engineering, Bollikunta, Warangal (A.P), India

* E-mail of the corresponding author: bapuji.vala@gmail.com

Abstract

The performance of distributed networks depends on collaboration among distributed entities. To enhance security in distributed networks, such as ad hoc networks, it is important to evaluate the trustworthiness of participating entities since trust is the major driving force for collaboration. The trust based security protocol based on a cross-layer approach attains confidentiality and authentication of packets in both routing and link layers of MANETs but it doesn't address few attacks like Bad Mouthing Attack, On-off Attack, and Conflicting Behavior Attack, Sybil Attack and Newcomer Attack. In this paper we present DAS, a protocol for reducing of the corruptive/malicious influences of Sybil attacks. Malicious users in general may create multiple identities with few trust relationships. Hence there is a disproportionately small gap in the graph between the Sybil nodes and the honest nodes. DAS exploits this property so as to bind the number of identities a malicious user can create. We simulate the effectiveness of DAS both analytically and experimentally.

Keywords: MANETs, Security Protocol, DAS, Malicious nodes, Cross Layer, Authentication

1. Introduction

In ad hoc networks, securing routing protocols is one of the fundamental challenges. While many secure routing schemes focus on preventing attackers from entering the network through secure key distribution or authentication and secure neighbor discovery, trust management can guard routing even if malicious nodes have gained access to the network. Trust management can effectively improve network performance and detect malicious entities. Therefore, trust management itself is an attractive target for attackers. If a malicious node can create several faked IDs, the trust management system suffers from the *Sybil attack* [19]. The faked IDs can share or even take the blame, which should be given to the malicious node. Most of the designs against such malicious behavior depend on the assumption that a certain fraction of the nodes in the system are honest. For instance, virtually all protocols for tolerating Byzantine failures assume that at least 2/3 of the nodes are honest. Thus, an effective defense against Sybil attacks would help in removal of a primary practical obstacle to collaborative tasks on peer-to-peer (P2P) and other decentralized systems.

1.1 Problems with using Trusted Third Party (TTP)

A trusted third party can be used to control Sybil attacks easily, that issues and verifies credentials unique to an actual human being. For instance, the system may require users to register with government-issued smart cards or pan cards, and then the barrier for launching a Sybil attack becomes much higher. The trusted third party may also instead require a payment for each identity.

Unfortunately, there are many cases where such designs are not desirable. For instance, it may not be easy to select/establish a single entity that every user worldwide is willing to trust. Furthermore, the trusted third party can easily be a single point of failure, a single target for denial-of-service attacks, and also a bottleneck for performance, unless its functionality is it widely distributed. Requiring sensitive information or payment in order to use a system may scare away many potential users.

1.2 Decentralized Approaches Vs Centralized Approaches

Without a trusted central authority defense against Sybil attacks is much harder. Many decentralized systems today try to defend Sybil attacks by binding an identity to an IP address. However, malicious users can readily harvest (steal) IP addresses.

A malicious user can compromise a large number of end-user machines, thus creating a botnet of thousands of compromised machines spread throughout the Internet. Botnets in general are particularly hard to defend against because nodes in botnets are indeed distributed end users' computers. The investigations into Sybil attacks [21] showed that they cannot be prevented unless special assumptions are made.

The difficulty is from the fact that resource-challenge approaches, such as computation puzzles, require the challenges to be posed/validated simultaneously. Moreover, the adversary/misfeasor can potentially have significantly more resources than a typical end user. Puzzles that require human efforts, such as CAPTCHAs [23], can be reposted on the adversary's web site to be solved by other users seeking access to the site. Furthermore, these challenges must be performed directly instead of trusting someone else's challenge results, because Sybil nodes can vouch for each other. A more recent proposal [20] suggests the use of network coordinates [22] to determine whether multiple identities belong to the same user (i.e., have similar network coordinates).

1.3 DAS: A New defense Against Sybil Attacks

This paper presents DAS, a novel decentralized protocol that limits the corruptive influence of Sybil attacks, including Sybil attacks exploiting IP harvesting and even some Sybil attacks launched from botnets outside the system.

Identities are nodes in the graph and (undirected) edges are human-established trust relations (e.g., friend relations). The edges connecting the honest region (i.e., the region containing all the honest nodes) and the Sybil region (i.e., the region containing all the Sybil identities created by malicious users) are called attack edges. Our protocol ensures that the number of attack edges is independent of the number of Sybil identities, and is limited by the number of trust relation pairs between malicious users and honest users.DAS relies on a special kind of verifiable random walk in the graph and intersections between such walks. These walks are designed so that the small quotient cut between the Sybil region and the honest region can be used against the malicious users, to bound the number of Sybil identities that they can create. We will show the effectiveness of DAS both analytically and experimentally.

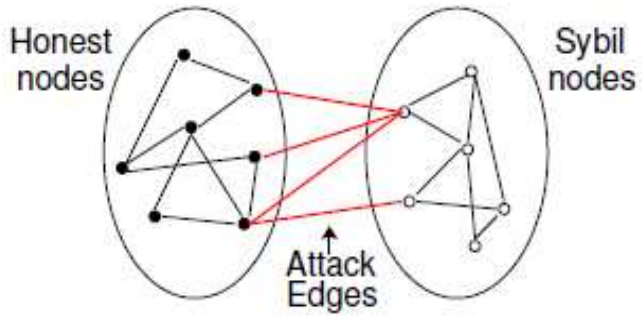

Figure.1. A Network with Honest and Sybil Nodes.

2. Model and Problem Formulation

In ad hoc networks, securing routing protocols is one of the fundamental challenges. While many secure routing schemes focus on preventing attackers from entering the network through secure key distribution or authentication and secure neighbor discovery, trust management can guard routing even if malicious nodes have gained access to the network.

The system has n honest human beings as honest users, and one or more malicious human beings as malicious users. By definition, a user is distinct. Each honest user has a single (honest) identity, while each malicious user has one or more (malicious) identities. To unify terminology, we simply refer to all the identities created by the malicious users as Sybil identities. Identities are also called nodes, and we will from now on use "identity" and "node"

interchangeably. All malicious users may collude, and we say that they are all under the control of an adversary.

Nodes participate in the system to receive and provide service (e.g., file backup service) as peers. Because the nodes in the system may be honest or Sybil, a defense system against Sybil attacks aims to provide a mechanism for a node V to decide whether or not to accept or reject another node S. Accepting S means that V is willing to receive service from and provide service to S. Ideally, the defense system should guarantee that V accepts only honest nodes. Because such an idealized guarantee is challenging to achieve, we aim at providing the following guarantees that, while weaker, are still sufficiently strong to be useful. The first guarantee is based on defining an equivalence [4] relation among accepted nodes. The equivalence relation partitions all accepted nodes into equivalence classes, called equivalence groups.

Notice that nodes that are rejected do not belong to any equivalence groups. An equivalence group that includes one or more Sybil nodes is called a Sybil group. The defense system provides a guaranteed bound on the number of Sybil groups, without necessarily knowing which groups are Sybil. If the defense system guarantees that the number of Sybil groups is at most some value g, then placing the file on nodes from g+1 different equivalence groups will ensure at least one good copy of the file. Another example is replicating a file that is not signed. As long as we obtain the file from 2g+1 nodes from 2g+1 different equivalence groups, the majority is guaranteed to have the correct file. In some other scenarios the bound on the number of Sybil groups depends on how "powerful" the adversary is.

A defense system may further bound the number of nodes accepted into each of the g Sybil groups. If the number of nodes in each Sybil group (or the size of the Sybil group) is at most w, then a node will accept at most g ·w Sybil nodes. To see the benefits of bounding both the number and size of the Sybil groups, consider our running example of replicating unsigned and signed files. Suppose we use a simple assignment that maps replicas to random nodes. If g · w is smaller than the number of honest nodes n, then from Chernoff bounds [24], the probability of having a majority of the replicas on honest nodes (as required for unsigned files) approaches 1.0 exponentially fast with the number of replicas.

3. DAS Design

In the network under consideration each pair of friends shares a unique symmetric secret key (e.g., a shared password) called the edge key. The edge key is used to authenticate messages between the two friends (e.g., with a Message Authentication Code). Because only the two friends need to know the edge key, key distribution is easily done out-of-band (e.g., via phone calls). A node can also revoke an edge key unilaterally simply by discontinuing use of the key and discarding it. A node informs its friends of its IP address whenever its IP address changes, to allow continued communication via the network. This IP address is used only as a hint. It does not result in vulnerability even if the IP address is wrong, because authentication based on the edge key will always be performed. If DNS and DNS names are available, nodes may also provide DNS names and only update the DNS record when the IP address changes.

In ad hoc networks, securing routing protocols is one of the fundamental challenges. While many secure routing schemes focus on preventing attackers from entering the network through secure key distribution or authentication and secure neighbor discovery, trust management can guard routing even if malicious nodes have gained access to the network.

The effectiveness of DAS relies on there being a limited number of attack edges (g). There are several ways the adversary might attempt to increase g:

- The malicious users establish social trust and convince more honest users in the system to "be their friends" in real life. But this is quite difficult to do on a large scale.
- A malicious user (Bob) who managed to convince an honest user (John) to be her friend creates many Sybil nodes, and then tries to convince John to also be friends with these Sybil nodes. But John only has a single edge key corresponding to the edge between Alice and Bob. As a result, all messages authenticated using that edge key will be considered by John to come from the same edge. Thus the number of attack edges remains unchanged.
- The adversary compromises a single honest node with degree d. Because d was already constrained (before

the node is compromised) within some constant by the user, g can be increased by at most some constant. On the other hand, the adversary will not be able to create further attack edges from the node because adding an edge to another honest user requires out-of-band verification by that user. When a user drops and then makes new friends, it is possible for the adversary with access to the old edge keys to "resurrect" dropped edges and hence further increase g. However, we expect such effect to be negligible in practice and if necessary, can be prevented by requiring out-of-band confirmation when deleting edges.

- The adversary compromises a small fraction of the nodes in the system. This will not likely increase g excessively due to the reasons above.
- The adversary compromises a large fraction of the nodes in the system. Here the system has already been subverted, and the adversary does not even need to launch a Sybil attack. DAS will not help here.
- The adversary compromises a large number of computers (i.e., creates a botnet), only some of which belong to the system.

The increase in g is upper bounded by some constant times the number of compromised computers which already belong to the system. The increase is not affected by the total size of the botnet. Although acquiring a botnet with many nodes may be relatively easy (e.g., in the black market), acquiring a botnet containing many nodes that are already in the system is more challenging

In summary, DAS is quite effective in limiting the number of attack edges, as long as not too many honest users are compromised. Relatively speaking, DAS is more effective defending against malicious users than defending against compromised honest users that belong to the system. This is because a malicious user must make real friends in order to increase the number of attack edges, while compromised honest users already have friends.

DAS requires each node S to register with all w nodes along each of its routes. A node Q along the route permits S to register only if S is one of the nodes that are within w hops "upstream". When the verifier V wants to verify S, V will ask the intersection point (between S's route and V's route) whether S is indeed registered. In this registration process, each node needs to use a "token" that cannot be easily forged by other nodes. Note that the availability of such tokens does not solve the Sybil attack problem by itself, because a malicious user may have many such tokens. A node will be accepted based on its token. This design assumed no IP spoofing, and was mainly suited for users with static or slowly changing IP addresses.

Our current design of DAS uses public key cryptography for the tokens. Each honest node has a locally generated public/private key pair. Notice that these public and private keys have no connection with the edge keys (which are secret symmetric keys). Malicious nodes may create as many public/private key pairs as they wish. We use the private key of each node as the unforgettable token, while the public key is registered along the random routes as a proof of owning the token. Note that we do not intend or need to solve the public key distribution problem, because we are not concerned with associating public keys to, for example, human beings or computers. The only property DAS relies on is that the private key is unforgettable and its possession can be verified.
A Sybil node may not follow the protocol and may arbitrarily manipulate the registry tables and witness tables. DAS is still secure against such attacks. To understand why and obtain intuition, it helps to consider the set of all registry table entries on all honest nodes in the system. For simplicity, assume that all honest nodes have the same degree d. Thus there are altogether, $n \cdot d \cdot w$ registry table entries in the system.

Consider a malicious node M and a single attack edge connecting an honest node A with M. Clearly, M can propagate to A an arbitrary registry table, thus polluting the w entries in A's registry table. Suppose A next forwards the registry table to B, who shifts the table downward and adds A as the first entry. Thus $w-1$ entries in B's registry table are polluted. Continuing this argument, we see that a single attack edge enables M to control $w+(w-1)+\ldots+1 \approx w^2/2$ entries system-wide. With g attack edges and even when gw approaches n, the total number of polluted entries ($gw^2/2$) is still less than half of the total number of entries ($n \cdot d \cdot w$). This provides some intuition why the number of accepted Sybil nodes is properly bounded even though the adversary may not follow the DAS protocol. The system has n honest human beings as honest users, and one or more malicious human beings as malicious users.

3. Evaluation

This section uses simulation to evaluate the guarantees of DAS. We choose to use simulation because it enables us to study large-scale systems. We use the model to instantiate three different graphs: a million-node graph with average node degree of 24, a 10000-node graph with average degree of 24, and a 100-node graph with average degree of 12. For space limitations, we leave to [27] a review of the model and the detailed parameters. We also focus on the million-node graph, and present only summary results for the other two graphs. All results below are for the million-node graph unless otherwise mentioned.

4.1 Results with No Malicious Users

We start by studying the basic behavior of DAS when there are no malicious users. Without malicious users, the only property we are concerned with is whether an honest verifier accepts an honest suspect. Probability of an honest node being successfully accepted. We move on to study the probability of the verifier V accepting the suspect S. For V to accept S, their routes must intersect and at least one intersection must be online. We do not directly model nodes being online or offline. Rather, we assume that as long as there are at least 10 intersections, the verification succeeds. Note that even when nodes are online only 20% of the time, the probability that at least one out of 10 intersections is online is already roughly 90% other two graphs. All results below are for the million-node graph unless otherwise mentioned.

4.2 Results with Sybil Attackers

Next we study the behavior of DAS when there are malicious users. In most security research, the term

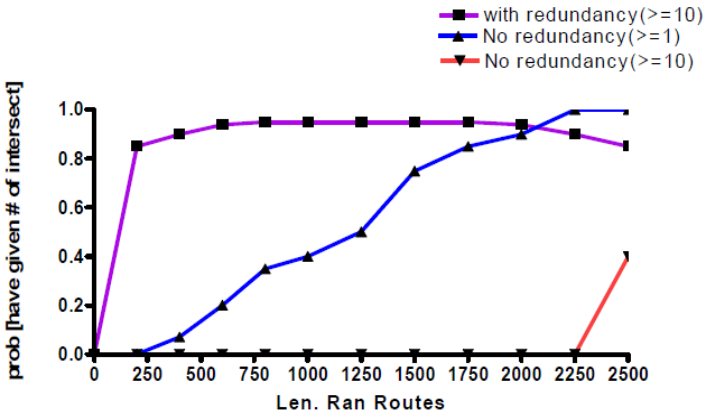

Figure.2. Probability of intersection.

Figure.2. Represents legend “with redundancy” means that each node performs random routes along all directions, while “no redundancy” means performing a single random route. The legend “(>= x)” means that we are considering the probability of having at least x distinct intersections. DAS corresponds to “with redundancy (>= 10)”.

“malicious user” typically refers to a single malicious user who does not assume additional identities.

In this paper, however, malicious users refer to powerful attackers who have the sophistication and computation power to launch Sybil attacks. For clarity, we use “Sybil attackers” to refer to these users in our evaluation. Each of these Sybil attackers can potentially create an unlimited number of “malicious users”.

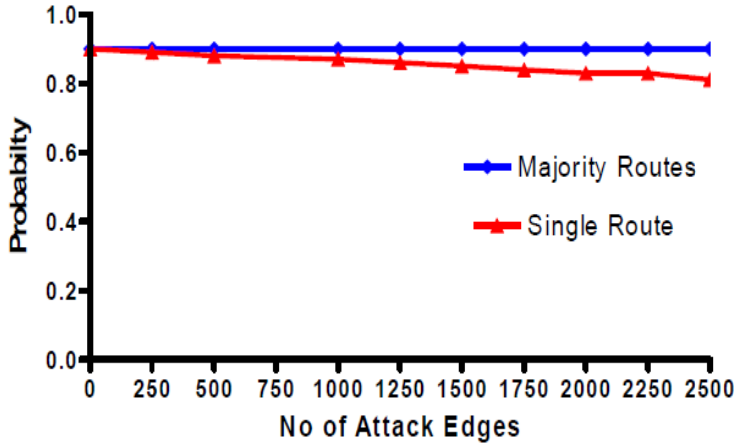

Figure.3. Probability of routes remaining entirely within the honest region.

For our experiments based on the million-node graph, we vary the number of attack edges g from 0 to 2500. When g = 2500, there are roughly 100 nodes marked as Sybil attackers. It is crucial to understand that just having 100 Sybil attackers in the system will not necessarily result in 2500 attack edges on average, each attacker must be able to convince 25 real human beings to be his friend. The hardness of creating these social links is what DAS relies on. In the presence of Sybil attackers, we are concerned with several measures of "goodness": (i) the probability that an honest node accepts more than $g \cdot w$ Sybil nodes; (ii) the probability that an honest node accepts another honest node; and (iii) the impact of Sybil nodes on estimating w.

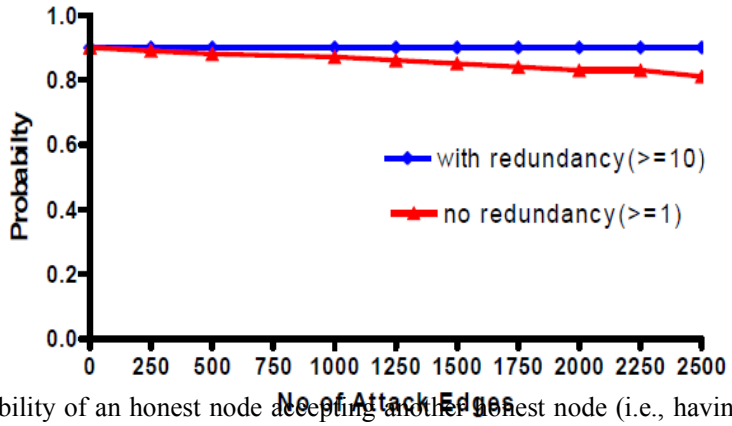

Figure.4. Probability of an honest node accepting another honest node (i.e., having at least a target number of intersections).The legends are the same as in Figure 3, and Sybil Guard corresponds to "with redundancy (>= 10)"

5. Conclusion

This paper presented DAS, a novel decentralized protocol for reducing the corruptive influences of Sybil attacks, by bounding both the number and size of Sybil groups. DAS relies on properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges. In all our simulation experiments with one million nodes, DAS ensured that (i) the number and size of Sybil groups are properly bounded for 99.8% of the honest users, and (ii) an honest node can accept, and be accepted by, 99.8% of all other honest nodes. Still a lot more dimensions have to be worked on and the research work is still wide open.

References

Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar *"Signature based Intrusion Detection forWireless Ad-Hoc Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003.*

Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis *"Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.*

Chin-Yang Henry Tseng, *"Distributed Intrusion Detection Models for Mobile Ad Hoc Networks" University of California at Davis Davis, CA, USA, 2006.*

Tarag Fahad and Robert Askwith *"A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.*

Panagiotis Papadimitratos, and Zygmunt J. Haas, *"Secure Data Communication in Mobile Ad Hoc Networks",IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.*

Ernesto Jiménez Caballero*,"Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem", 2006.*

A.Rajaram and Dr.S.Palaniswami *"A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks" in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No.1, 2009*

Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang*, "A secure incentive protocol for mobile ad hoc networks", Wireless Networks(WINET), vol 13,No. 5, October 2007.*

Liu, Kejun Deng, Jing Varshney, Pramod K. Balakrishnan and Kashyap "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, May 2007.

Li Zhao and José G. Delgado-Frias *"MARS:Misbehavior Detection in Ad Hoc Networks", in proceedings of IEEE Conference on Global Telecommunications Conference,November 2007.*

A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha "Threshold-based Intrusion Detection in Adhoc Networks and Secure AODV" Elsevier Science Publishers B. V., Ad Hoc Networks Journal (ADHOCNET), June 2008.

S.Madhavi and Dr. Tai Hoon Kim *"An Intrusion Detection System In Mobile Ad hoc networks" International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.*

Afzal, Biswas, Jong-bin Koh,Raza, Gunhee Lee and Dong-kyoo Kim, *"RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks", in proceedings of IEEE Conference on Wireless Communications andNetworking, pp.2313-2318, April 2008.*

Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam, *"Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", in proceedings of World Academy Of Science, Engineering And Technology, Vol. 36, pp.1373-1378, December 2008.*

Meka, Virendra, and Upadhyaya*, "Trust based routing decisions in mobile ad-hoc networks" In Proceedings of the Workshop on Secure Knowledge Management, 2006.*

Muhammad Mahmudul Islam, Ronald Pose and Carlo Kopp, *"A Link Layer Security Protocol for Suburban Ad-Hoc Networks", in proceedings of Australian Telecommunication Networks and Applications Conference, December 2004.*

[17] Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou and Kefei Chen *"Efficient Link Layer Security Scheme for Wireless Sensor Networks" Journal of Information And Computational Science, Vol.4, No.2,pp. 553-567,June 2007.*

C. Dellarocas, *"Mechanisms for coping with unfairratings and discriminatory behavior in online reputation reporting systems," in Proceedings of ICIS, 2000.*

J. Newsome, E. Shi, D. Song, and A. Perrig, *"The Sybil attack in sensor networks: Analysis and defenses,"* in Proceedings of the third International Symposium on Information Processing in Sensor Networks (IPSN),2004

R.Bazzi and G. Konjevod. *On the establishment of distinct identities in overlay networks.* In ACM PODC, 2005.

J. Douceur. The Sybil attack. In IPTPS, 2002.

T. S. E. Ng and H. Zhang. *Predicting internet network distance with coordinates-based approaches*. In IEEE INFOCOM, 2002.

L.Von Ahn, M. Blum, N. J. Hopper, and J. Langford. *CAPTCHA: Telling humans and computers apart*. In Eurocrypt, 2003.

M. Mitzenmacher and E. Upfal. *Probability and Computing*. Cambridge University Press, 2005.

Haifeng Yu et al, "*Defense against Sybil attacks via Social Networks*", SIGCOMM 2006, Pisa, Italy.

Arai, T., Aiyama, Y., Sugi, M. & Ota, J. (2001), "Holonic Assembly System with Plug and Produce", *Computers in Industry* 46, Elsevier, 289-299.

Bell, G.A., Cooper, M.A., Kennedy, M. & Warwick, J. (2000), "The Development of the Holon Planning and Costing Framework for Higher Education Management", Technical Report, SBU-CISM-11-00, South Bank University, 103 Borough Road, London, SE1 0AA.

Bongaerts, L. (1998), "Integration of Scheduling and Control in Holonic Manufacturing Systems", *PhD Thesis*, PMA Division, K.U.Leuven.

Deen, S.M. (1993), "Cooperation Issues in Holonic Manufacturing Systems", *Proceedings of DIISM'93 Conference*, 410-412.

Techawiboonwong, A., Yenradeea, P. & Das, S. (2006). A Master Scheduling Model with Skilled and Unskilled Temporary Workers", *Production Economics* 103, Elsevier, 798-809.

Valckenaers, P., Van Brussel, H., Bongaerts, L. & Wyns, J. (1997), "Holonic Manufacturing Systems", *Integrated Computer Aided Engineering* 4(3), 191-201.

Van Brussel, H., Wyns, J., Valckenaers, P., Bongaerts, L. & Peters, P. (1998), "Reference Architecture for Holonic Manufacturing Systems: PROSA", *Computers in Industry* 37(3), 255-274.

R. Naveen Kumar is a Ph.D. candidate, Department of Informatics Kakatiya University Warangal (A.P), India. He has 14 years of teaching experience. His interests include: Mobile Ad Hoc Networks Security Vulnerabilities and Key management, Cross Layer Design. E-mail: naveensmitha@gmail.com

V. Bapuji is currently pursuing Ph.D. degree in Computer Science at Kakatiya University Warangal (A.P), India. He has 12 years of teaching experience in Post Graduate level. His research interests include Mobile Ad Hoc Networks Security, Soft Computing, and Design efficient accurate reliable low cost IDS. His work focuses on the security and fault tolerance of routing protocols, with an emphasis on solutions to support Mobile Ad hoc Networking. E-mail: bapuji.vala@gmail.com

Dr. A. Govardhan is a Professor, Department of computer science and Engineering at Jawaharlal Nehru Technological University (JNTUH) Hyderabad (A.P), India. His research interests are in the area of Mobile Computing, Data management in wireless mobile environments and Data Mining. He has served on several program

committees of conferences in the area of mobile computing, data management and sensor networks. He is a Senior Member of IEEE, ACM and various organizations. He has organized several workshops, delivered numerous tutorials at major IEEE and ACM conferences, and serves as editor of several journals and magazines. E-mail: govardhan_cse@yahoo.co.in

S.S.V.N. Sarma was a Professor (From 1975 to 2010). He has 40 years of experience and worked as Head, Department of Informatics, Chairman Board of Studies, and Dean Faculty of Science, Kakatiya University, Warangal (A.P) India. Presently he is working as a Dean, Academic Affairs at Vaagdevi College of Engineering, Bollikunta, Warangal (A.P), India. His current research interests include Distributed systems, Mobile computing, Computer networks, Computer security, and Performance evaluation. He has published over 120 refereed articles in these areas. He has organized several workshops, delivered numerous tutorials at major IEEE and ACM conferences, and serves as Editor of several International/National journals and magazines. He is a fellow member of professional organizations. E-mail: ssvn.sarma@gmail.com