A Generalized Trust Framework for Mobile Ad Hoc Networks

Revathi Venkataraman[1], M. Pushpalatha[1], and T. Rama Rao[2]

[1] Assistant Professor, Computer Science & Engg
[2] Professor, Telecomunication Engg
revathi@ktr.srmuniv.ac.in, ramarao@ieee.org

Abstract. Mobile ad hoc networks (MANET) are formed when two or more nodes come within the communication range of each other. Since the wireless range is very short, all the nodes in the network have to extend their complete co-operation for efficient functioning of the network. This paper proposes a generalized trust framework for any ad hoc routing protocol to curb selfish and malicious nodes in a MANET. The trust relationships existing between the nodes determine the routing path to be taken for data transfer. The trust framework is combined with any MANET routing algorithm. The performance analysis of this framework is currently done with two reactive protocols. Jointly, they form a trusted network to curb various attacks originating in the ad hoc network. This type of a trusted framework established in a MANET, would be most suited for tactical environments.

1 Introduction

Security is one of the major issues to be considered in the deployment of MANETs in a tactical network environment. Since, today's world is moving toward Network-Centric Warfront [1], the requirements and functionalities of ad hoc networks are much more than their wired counterparts. MANETs should provide all services like routing, data forwarding, resource availability which are typically offered by infrastructure-based networks, in a most secure environment. In addition, the participating entries in the network should be capable to self-organizing among themselves in a dynamically changing topology with limited resources. The absence of centralized infrastructure or server component in mobile ad hoc networks poses the greatest security challenge [2]. Since no monitoring or detection software can be deployed for the network, the mobile devices which form the network have to take care of routing, security and all other server functionalities. Hence, all mobile devices are expected to extend their co-operation in exchanging routing information, forwarding of data packets etc. It is easily possible that after the deployment of these mobile devices, some of the nodes may be implanted by enemies in a tactical environment [1]. These nodes may behave maliciously, disrupting the networking services. Therefore, it is very essential to safeguard the ad hoc networks which are deployed in a tactical environment. Effective solutions to these security issues need to be proposed for widespread deployment of mobile ad hoc networks.

N. Meghanathan et al. (Eds.): NeCoM, WiMoN, and WeST 2010, CCIS 90, pp. 326–335, 2010.

The wireless links are more susceptible to various types of attacks like passive eavesdropping, active modification of messages, disruption of service, replay attacks and impersonation attacks [2]. The compromised nodes makes use of the unreliable links and dynamic topology of ad hoc networks and introduce inconsistencies in the routing table information exchange. It is very difficult to detect these nodes because there is no central server component wherein key management and monitoring software can be installed. Hence, detection of attacks and countermeasures to be taken in the midst of these attacks will be very complex. Establishment of trust relationship between the nodes will lead to the detection of these attacks and isolation of compromised nodes [2].

To curb selfish behavior of nodes in mobile ad hoc networks, three broad strategies are identified: reputation-based methods, credit-based methods and game theory solutions [3]. In reputation-based schemes, the neighboring nodes are observed and their behavior is quantified and used for routing and packet forwarding. In credit-based techniques, the co-operating nodes are benefited from their benevolent behavior. In game-theory based approaches, the entire forwarding process is modeled as a game and individual participants are expected to find an optimal strategy.

This paper is an initiative towards providing a security solution which spans the entire protocol stack of a MANET. The attacks under consideration for this paper are black holes, grey holes and flooding attacks. A comprehensive trust framework is suggested which will improve the efficiency of the network even in the presence of these attacks. The rest of the paper is organized as follows. Section 2 describes the related works and literature review done on security issues in mobile ad hoc networks, as well as various trust establishment schemes. Few works on flooding attacks prevention and wormhole detection strategies are also analyzed. Section 3 briefs about the proposed strategies to prevent the abovementioned subset of attacks. A Trust architecture to be incorporated in each mobile node is discussed. Section 4 describes about the performance analysis of the proposed methods. Section 5 mentions about further enhancements to be made to the trust model.

2 Related Works

The lack of trusted environment in an ad hoc network results in many security lapses. This is considered as one of the major concerns in the large scale deployment of ad hoc networks [4]. Trust establishment algorithms [5, 6, 7] have been developed which addresses few of the security attacks possible in an ad hoc network. The participating nodes should know in advance regarding the type of security attack in the network and run the corresponding algorithm to detect the misbehaving nodes in the network. Most of the techniques are suited to prevent or detect a specific type of attack. These schemes do not provide any comprehensive framework for securing the ad hoc network resources.

The Dynamic Source Routing(DSR) protocol for dependable routing as presented in [8] has the possibility of flooding and sinkhole attacks in the network. Again, this scheme is suited for DSR and it has to be customized for other proactive and reactive protocols. An improvised protocol version is presented in [9] for DSR and Ad hoc On-demand Distance Vector (AODV). Some of the cryptographic protocol

schemes [10, 11, 12] presented have the overheads associated with the secure routing at all times. Also, distribution of certificates and key management is again an issue in mobile ad hoc networks. The presence of a server or a central monitoring component is inevitable in these schemes. Computational overheads involved in executing a cryptographic algorithm are considerable. The battery power and computational overheads assume great importance in a resource constraint MANET environment. These schemes will be impractical for deployment of wireless ad hoc networks in real world.

Resisting flooding attacks in ad hoc networks as in [13, 14] describes two flooding attacks: Route Request (RREQ) and Data flooding attack. In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. A single threshold is set up for all the neighbor nodes. The given solution is neighbor suppression. In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated. . Similar solutions are proposed in [15] where a rate-limitation component is added in each node. This component monitors the threshold limit of request packets sent by the neighboring nodes and accordingly, drops the packets if the limit is exceeded. Flooding by data packets is not addressed.

The work presented in [16, 17, 18] provides a generalized trust metric scheme to be used for neighbor evaluation. The direct trust refers to the trust computed for all the nodes which are adjacent to the evaluating node. Recommendation trust is an indirect trust given by a node i, about node j to a node k. Two schemes are presented: distance semiring, which aggregates the trust from one node to another along a particular path; path semiring, which aggregates the trust from one node to another along different (parallel) paths. Even though these schemes are useful in collecting a global trust value for a particular node in the network, the overheads associated with these techniques needs to be analyzed. And the practical limitations of computing a trust value for a node, taking the feedback of every other node in the network needs to be studied in an ad hoc environment where all the information are localized.

Hence, our proposed system considers only the direct trust values based on the experience of the node with its neighbors. The trust concept was introduced in DSR protocol and its performance analyzed in [19]. Furthermore, a proposal for flooding attack prevention using the trust scheme is made in [20]. Initially, at the time of initiation of an ad hoc network all the nodes will be strangers with unknown trust values. Later, the observations and behaviors of the neighboring nodes are recorded and an analyzed and the neighboring nodes are categorized.

3 Proposed Model

The trust establishment algorithms will run below any MANET routing algorithm. Fig.1 shows the security issues in a wireless protocol stack. Every participating node in an ad hoc network will be fortified with the trust architecture as shown in Fig.2. The trust relationships between individual nodes in an ad hoc network may belong to any type as shown in Table 1.

Table 1. Trust Relationships existing between ad hoc nodes

Relationship: Node i→ Node j	**Trust significance**
Stranger	The neighbor node is not evaluated. Default value
Acquaintance	Neighbor node is evaluated for relatively short duration. Upgraded from stranger status.
Friend	Neighbor node is one among the trusted nodes in the network. The relationship is evaluated over a period of time. Upgraded from acquaintance.
Malicious	Blacklisted neighbor nodes. These nodes are evaluated to over a short duration and their co-operation is not satisfactory. Degraded from stranger.

At the time of initiation of the ad hoc network, all the nodes will be strangers to each other. At that time, no routing packets exchange or data transfer would have taken place. Hence, the nodes in the network would not have had a chance to evaluate their neighbors. Once, the first request for data transfer comes in a participating node, it initiates the ROUTE DISCOVERY process by broadcasting the RREQ message. The trust estimator in the node will be in promiscuous mode overhearing the transmission of the neighboring nodes. The counter which records the RREQ message broadcast will be incremented or decremented based on the behavior of the neighboring node. Similarly, black hole attacks of the neighboring nodes can be detected. Table 2 lists the metrics for estimating the trust relationship of a neighboring node.

The overall trust relationship with a neighboring node is computed by performing the aggregation of individual metrics. The Ordered Weighted Averaging(OWA) operator is used for aggregation of individual constraints.

Table 2. Trust metrics defined in an individual node

Trust Metrics
Number of RREQ packets successfully forwarded
Number of DATA packets successfully forwarded
Number of instances with matched message digest values in packet transmission
Number of RREQs received from the neighboring node
Number of DATA packets received from the neighboring node
Time taken to respond to a RREQ message

$$OWA(T_1,T_2.....T_n) = \sum_{j=1}^{n} w_j T_{\sigma(j)} \quad (1)$$

Where T1,T2…..Tn are individual trust metrics, wj are positive weights associated with each trust metric and σ(j) is the permutation ordering of the metric.Wj > 0 and $\sum_{j=1}^{n} w_j = 1$. The purpose of assigning weighted trust metric is to give different weights to different trust metric. The aggregated trust value is normalized within limits (0 to 1). The normalized trust value from Eqn 2 will determine whether the neighboring node is a friend, acquaintance, stranger or malicious as shown in Table 3.

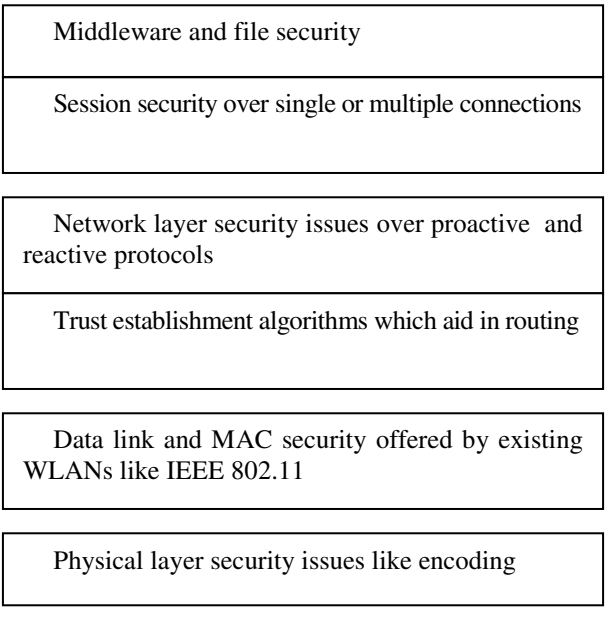

Fig. 1. Security Issues in a wireless ad hoc protocol stack

$$\text{Normalized trust } T = \frac{(A_c - A_{\min})(L_{\max} - L_{\min})}{A_{\max} - A_{\min}} + L_{\min} \quad (2)$$

Where A_c - current aggregated trust
$A_{\min}$ - minimum possible aggregated trust
$L_{\max}$ - 1
$L_{\min}$ - -1
$A_{\max}$ - maximum possible aggregated trust

These computed trust values are stored along with routing information in the route cache table. These observations are used in choosing the right path for data transmission. After

discovering the routes and updating the information in the route cache, the data transfer will be initiated. Before transmission of data packets, a message digest is computed for the packet and sent to the neighboring node. The current node will switch to promiscuous mode and listen to the packet transmission of the neighboring node. It will recompute the message digest of the packet transmitted from neighboring node. If the values match, no content modification of the packet is done by the neighboring node. Accordingly, another counter keeps track of this behavior of the node and records it.

Some of the neighboring nodes may act malicious by frequently involving ROUTE DISCOVERY process. These nodes may use the stale route table information and initiate the route discovery process for destination nodes which never exist in the network. They may involve in RREQ Flooding attacks. Hence, all the neighboring nodes which receive the RREQ will remain in the active mode participating in the route discovery process. This scenario will exhaust the network resources; drain the battery power, thereby reducing the battery life of the ad hoc devices. To curtail flooding attacks, the proposed trust model in the ad hoc node, monitors this activity. Any node can accept only a certain number of RREQs from its neighboring node. If it exceeds the RREQ threshold limit set for its trust relationship, which it maintains with the current node, further RREQs will be destroyed. A similar setup is used for DATA Flooding attacks by the malicious nodes. A neighboring malicious node may be cooperative in route discovery process. Once the data transfer begins, it may start sending junk packets for transmission. Even though, the content of the packet can not be viewed at the network layer, depending on the volume of data transfer, restrictions can be applied over the incoming traffic from neighboring node. To prevent DATA Flooding, incoming packets for data transfer can be accepted from a neighboring node till a certain threshold is reached. Since the packet arrival from a neighboring node is assumed to follow a randomized Poisson distribution, any deviation from the distribution pattern indicates malicious intention of the neighboring node and their behavior is recorded. The cumulative probability Pn of getting n junk packets from a neighboring node is expressed using Poisson distribution in Eqn 3.

$$P_n = \sum_{k=0,n} e^{-\lambda} \lambda^n / k! \qquad (3)$$

where k is the number of times incoming packets were processed from the neighboring node at a constant rate λ.

Table 3. Trust threshold limits

Relationship with neighboring node	Trust Threshold (normalized)
Friend	> 0.75
Acquaintance	>0.3 and < 0.75
Stranger	<0.3 and positive
Malicious	-1

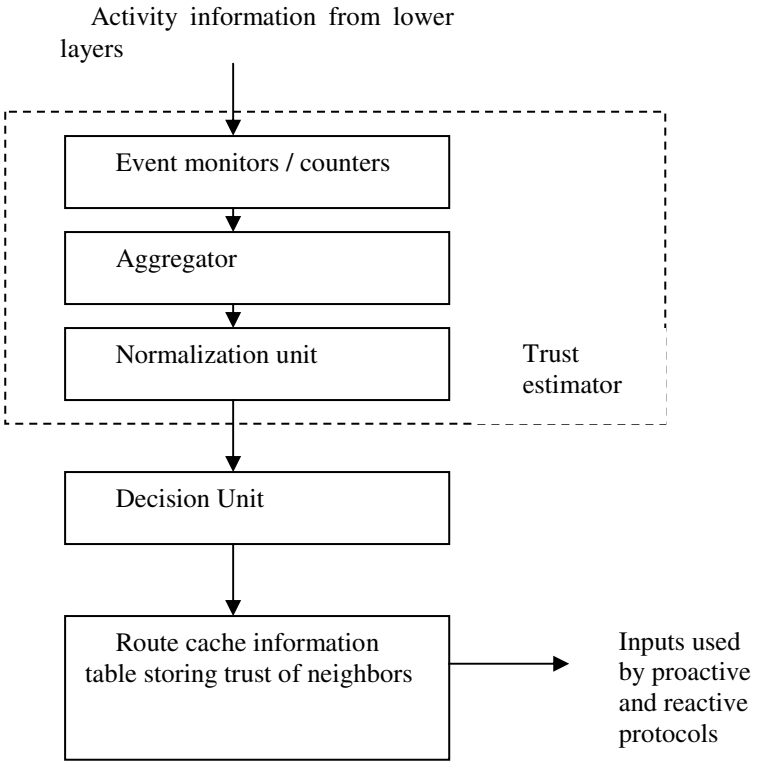

Fig. 2. Trust Architecture in an individual node

4 Simulations and Performance Analysis

4.1 Test 1: Few Black Holes as Neighbors over DSR Protocol

In a standard MANET running DSR protocol, compromised nodes are introduced into the network. These intermediate malicious nodes involve in active attack by receiving the data packets, not meant for them and simply not forwarding them. Simulations are carried out in OPNET Modeler in a 500 X 500 Sq.m area and the mobility model chosen is Random Waypoint. There are 25 nodes moving about with a speed of 20m/s and the transmitted power of these nodes is 1 mW. Fig.3 compares the throughput of standard DSR and modified DSR by varying the number of malicious nodes in the network. The modified DSR copes up well in an environment where the number of malicious nodes in the network is less than six out of twenty five. The performance of the trusted network is analyzed with six different scenarios as shown in Fig.4. In all the scenarios except scenario 5, the percentage of malicious nodes in the network is 40%. Scenario 1 represents a network by decreasing the node density in an area. Scenario 2 is with increasing node mobility speed. Scenario 3 is with slight increase in transmitted power of the participating nodes. Scenario 4 represents a

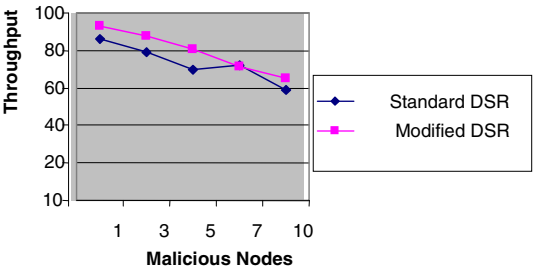

Fig. 3. Comparison of Throughput by varying malicious nodes in scenario 25 nodes, 20m/s, 20 connections

network with increased number of nodes. In scenario 5, number of malicious nodes is decreased to 5%. Scenario 6 represents an extreme case with many failed connections. In all these environments, the trusted network over DSR protocol offers increased throughput compared to standard DSR. The neighboring nodes behaving as black holes are detected and an alternate path is found to destination over the trusted nodes.

4.2 Flooding Attacks over AODV

Simulations are carried out over a mobile ad hoc network running AODV protocol. The simulation parameters are same as Test1. In default scenario, four nodes are made malicious by making them to transmit RREQ packets frequently with different identifiers which are meant for various destinations not existing in the network. Fig.5 shows the delay of packet transfer in seconds for the entire network. In modified AODV, all the nodes in the network run the trust establishment algorithm and evaluate their neighbors. Based on their observations, they accept RREQ packets from their neighbors depending on their respective thresholds. If their neighbors exceed their limit, their RREQ packets are dropped. The reduction in delay of packet transfer is accounted for by the involvement of the nodes in data transfer rather than participating in the RREQ flooding traffic caused by malicious nodes. From Fig.4, we can conclude that the superfluous routing packets sent by malicious nodes are immediately destroyed by its neighboring node.

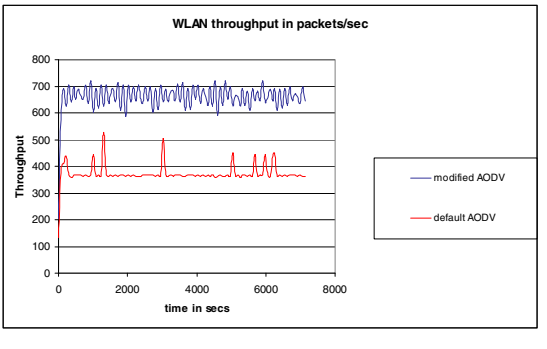

Fig. 4. Routing traffic received from a malicious node in packets/sec

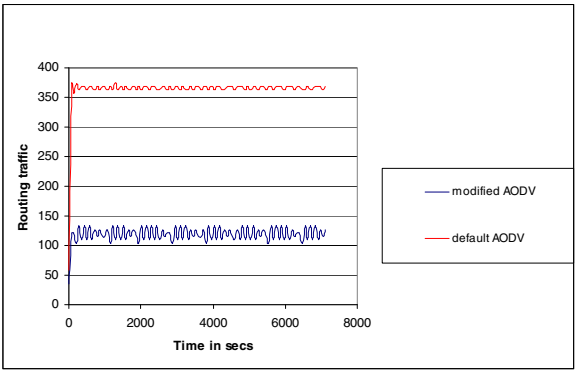

Fig. 5. WLAN throughput in packets/sec

Fig. 5 shows the increase in the WLAN throughput using the modified AODV. Thus, adding a trust establishment framework in every mobile node in an ad hoc network, curtails flooding attacks and improves the performance of the WLAN networks.

5 Conclusion

Wireless ad hoc networks are more prone to security attacks because of the vulnerable environment, frequently changing topologies and absence of centralized infrastructure. Since security is one of the major issues to be considered in the large scale deployment of mobile ad hoc networks, our work is an initiative towards the development of a foolproof trust model which can detect and isolate a wide set of security attacks possible in an ad hoc environment.

A generalized trust framework is formulated and every node in the network will incorporate the trust architecture. The neighbor behavior and relevant events are observed and given as input to the routing algorithms. These trust information help in choosing the best path for data transfer in an ad hoc communication. In addition, the nodes protect themselves from their malicious neighbors by retaining their resources like power and computation time. Our trust model currently detects *black holes*, *grey holes* and *flooding attacks* in the neighborhood. The efficiency of this model is tested over DSR and AODV protocols.

Acknowledgements. We sincerely thank our colleague Mr.K.Senthil Kumar, Assistant Professor, Dept of CSE, SRM University for his valuable suggestions in the preparation of this paper.

References

[1] Burbank, J.L., Chimento, P.F., Haberman, B.K., Kasch, W.T.: Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communications Magazine 44(11), 39–45 (2006)

[2] Buttyán, L., Hubaux, J.-P.: Security and Co-operation in wireless networks. Cambridge University Press, Cambridge (February 2007)
[3] Yoo, Y., Agrawal, D.P.: Why Does It Pay To Be Selfish In A Manet? IEEE Wireless Communications (December 2006)
[4] Conti, M., Giordano, S.: Multihop Ad Hoc Networking: The Reality. IEEE Communications Magazine 45(4), 88–95 (2007)
[5] Li, J., Kato, J.: Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine (April 2008)
[6] Sun, Y., Han, Z., Liu, K.J.R.: Defense of trust management vulnerabilities in distributed networks. IEEE Communications Magazine (February 2008)
[7] Sun, Y., Yu, W., Han, Z., Liu, K.J.R.: Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc networks. IEEE JSAC 24(2) (February 2006)
[8] Pirzada, A.A., Datta, A., McDonald, C.: Incorporating Trust and Reputation in the DSR protocol for Dependable Routing. Computer Communications, Special issue on Internet Communications Security 29, 2806–2821 (2006)
[9] Pirzada, A.A., Datta, A., McDonald, C.: Performance Comparison of Trust-based reactive routing protocols. IEEE Transactions on Mobile Computing 5(6) (June 2006)
[10] Papadimitratos, P., Haas, Z.J.: Secure Data Communication in Mobile Ad hoc Networks. IEEE JSAC 24(2) (February 2006)
[11] Papadimitratos, P., Haas, Z.J., Samar, P.: The Secure Routing Protocol (SRP) for Ad Hoc Networks, IETF Internet Draft (March 2004), http://www.potaroo.net/ietf/idref/draft-papadimitratos-secure-routing-protocol
[12] Zhou, L., Haas, Z.J.: Securing Ad hoc Networks. IEEE Networks 13(6), 24–30 (1999)
[13] Yi, P., Dai, Z., Zhong, Y., Zhang, S.: Resisting Flooding Attacks in Ad Hoc Networks. In: International Conference on Information Technology, Coding and Computing, ITCC 2005, April 2005, vol. 2, pp. 657–662 (2005)
[14] Ping, Y., Yafei, H., Yiping, B., Shiyong, Z., Zhoulin, D.: Flooding Attacks and defence in Ad hoc networks. Journal of Systems Engineering and Electronics 17(2), 410–416 (2006)
[15] Balakrishnan, V., Varadharajan, V., Tapakula, U., Gaup Moe, M.E.: Mitigating Flooding attacks in Mobile Ad hoc Networks Supporting Anonymous Communications. In: Proceedings of the 2nd International Conference on Wireless and Ultra Wideband Communications, Auswireless, p. 29 (2007)
[16] Theodorakopoulos, G., Baras, J.S.: On trust models and trust evaluation metrics for ad hoc networks. IEEE Journal on Selected Areas in Communications 24(2), 318–328 (2006)
[17] Theodorakopoulos, G., Baras, J.S.: A Testbed for Comparing Trust Computation Algorithms. In: Proceedings of the 25th Army Science Conference, Orlando, FL, November 27-30 (2006)
[18] Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: WiSe 2004: Proceedings of the 3rd ACM workshop on Wireless security, PA, pp. 1–10 (2004)
[19] Venkataraman, R., Pushpalatha, M.: Security in Ad Hoc Networks: An extension of dynamic Source Routing in Mobile Ad Hoc Networks. In: Proceedings of the 10th IEEE International Conference on Communication Systems (2006)
[20] Venkataraman, R., Pushpalatha, M., Khemka, R., Rao, T.R.: Prevention of Flooding attacks in Mobile Ad hoc Networks. In: ICAC3 2009: Proceedings of the International Conference on Advances in Computing, Communication and Control, January 2009, pp. 525–529 (2009) ISBN:978-1-60558-351-8