

A Survey of Reputation Based Schemes for MANET

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom St. Liverpool, L3 3AF, UK

S.Abbas@2008.ljmu.ac.uk, M.Merabti@ljmu.ac.uk, D.Llewellyn-Jones@ljmu.ac.uk

Abstract— In multihop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance. Reputation, or trust based models are one of the most promising approaches to enforce cooperation and discourage node misbehaviour. Reputation is calculated through direct interactions with the nodes and/or indirect information collected from neighbours. Reputation is evolved on each node through monitoring or observing its direct interactions and a node can trust its direct information more than the indirect information. Since the monitoring component of a reputation based system has a substantial effect on its accuracy and reliability, we classify reputation based schemes based on their monitoring component: as using either active or passive acknowledgments. We survey and categorize reputation based schemes according to their passive and active acknowledgment monitoring techniques. Finally, we discuss their advantages and disadvantages with other related issues in the current models.

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a collection of nodes forming a temporary or permanent network without relying on any centralized architecture or control. Nodes can join or leave the network at any time and they can freely roam across the network. The avoidance of a centralized architecture also augments the MANET's ability to support a wide variety of applications on low cost hardware with less time required to set up infrastructure. Due to these flexibilities, it is tempting to use MANET in situations where there does not exist a pre-deployed infrastructure or where it is costly to deploy an infrastructure such as in disaster relief scenarios, search and rescue operations, vehicular networks, casual meetings, campus networks, robot networks, and so on.

MANETs were originally introduced as closed or managed networks that belonged to a single entity or organization called an offline authority, such as the military. In such networks end-users have a pre-established relationship and work under this offline authority. The offline authority usually does the initial set up procedures, for example to allot keys or certificates to nodes, and to allocate initial trust to the nodes, before network deployment. As nodes belong to a single authority and all have

a common objective, they are therefore motivated to cooperate. However, the proliferation of mobile communication devices such as laptops, PDAs, cell phones and other intelligent radio devices may produce a fully self-organized mobile ad hoc network. End-users come together to form a network in a purely ad hoc manner. Users are usually strangers without having any relationship and nodes have no pre-established security associations. They have different interests and objectives and they are therefore sharing their resources for the sake of global connectivity. The lack of a Trusted Third Party (TTP) and the untrusted users in a fully self-organized MANET causes the following security problems, as identified by McDonald *et al.* [1].

- Fully self-organized MANETs are open in nature; just like the Internet, nodes can join and leave the network at random. Openness attracts selfish and malicious users.
- Each end-user will be its own authority domain, and is therefore responsible for accomplishing distributed network functionalities, such as packet forwarding for other nodes or generating and maintaining its own keying material.
- There will always be a threat of active insider attacks in the network.
- As Douceur [2] pointed out, in the absence of an offline TTP, a node can create and control more than one identity without any cost or difficulty, termed as a Sybil attack. As a result, a node can join the network every time under different identities and hence it will be difficult to hold malicious nodes accountable for their actions.

Routing in MANETs is based on the multihop assumption [3], which shouldn't cause any problems in closed or managed MANETs where nodes belong to a single authority. However, this assumption may not be properly followed in a fully self-organized open MANET where nodes have their own domains and objectives. Since data transmission is the most expensive function in a wireless environment as compared to other functions such as data processing, nodes are naturally reluctant to spend their precious resources to forward other nodes' packets and can therefore exhibit selfish or sometimes malicious behaviour in open MANET environments. This

could potentially lead to network partitioning¹ and network performance degradation. Some authors, such as Agrawal *et al.* [4], have shown that a small percentage of selfish/malicious nodes can disrupt the whole network and severely degrade network performance. One can object that regular users don't usually have the appropriate skills and knowledge to modify the software or hardware functionalities for their own goals or interests and act selfishly. Hubaux *et al.* [5] answers this by pointing out that "criminal organizations can have enough interest and resources to reverse engineer a node and sell tampered nodes with modified behaviour on a large scale."

To enforce cooperation and discourage misbehaviour of nodes, three major models have been developed: a) Reputation based, b) Trust based and c) Credit based models, as shown in Figure 1. By utilizing the past behaviour of end-users, reputation and trust based schemes enable a node to decide whether other nodes are trustworthy and cooperative. Eventually nodes having high reputation or trust are given services and nodes having low reputation or trust are isolated from the network. In credit based schemes nodes usually pay for services; payments are made in the form of virtual currency. Nodes are buyers and/or sellers of the packet forwarding services. Nodes require credit to forward their packets. Credit based schemes have some issues that make them impractical for use in MANETs. Firstly, they are not scalable due to the central virtual bank. Secondly, these models need some form of tamper proof hardware on each node. Reputation or trust based models on the other hand do not need any centralized entity, such as a virtual bank, or any tamper proof hardware. As a consequence they can be implemented in a distributed manner to increase scalability, making them much more suitable for use in MANETs.

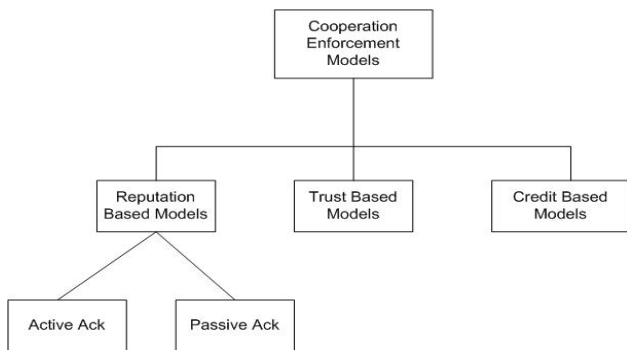


Figure 1: Cooperation Enforcement Schemes in MANETs.

A reputation based system collects first-hand or direct information by monitoring its immediate neighbours for direct interactions. To strengthen a node's decision regarding another node's behaviour, whether selfish or benign, second-hand

¹ By partition here we mean logical partitioning, which is not like topological partitioning (physical). These logical partitions cause service holes in the network.

information is collected from the deciding node's neighbours. However more weight is given to the direct interaction information, to mitigate the possibility of a neighbour node being deceitful.

The core part of the reputation based models is monitoring or observation of one hop neighbours. Due to the fact that a node can trust nobody but itself, it gives more weight to direct observations, which are called first hand information. The more perfect and reliable the monitoring component is the more accurate and efficient the detection of a misbehaving node will be. However, due to the complex and unpredictable nature of a mobile ad hoc network, it is very difficult to have a perfect monitoring system at low cost (where cost may be measured as energy or some other metric). In this document we have tried to ramify reputation schemes based on the monitoring components that can be referred to as active and passive acknowledgments. Both have their own advantages and disadvantages. In this document we will discuss the most famous reputation based schemes developed for mobile ad hoc networks. We categorize them, as well as discussing the pros and cons of the existing models and some other related issues that will need to be addressed in future research.

The rest of the document is organized as follows. In Section II we will survey reputation based schemes according to passive and active acknowledgments. In Section III, we summarize features and limitations of the surveyed schemes, highlight the advantages and disadvantages of both passive and active acknowledgments, and propose some future research directions. The document is concluded in Section IV.

II. REPUTATION BASED SCHEMES

A. The Rationale

Reputation based models consider the past history of interactions and based on this they enable nodes to identify cooperative (trusted) or uncooperative (untrusted) nodes. Nodes build up subjective reputation from their direct interaction experiences. These histories are made visible to the new interacting nodes in the form of second hand reputation information. However, nodes can use both direct and indirect experience to better evaluate the interacting nodes. Visible past histories are of significant importance in building reputation in the network. According to Friedman *et al.* [6], history is very beneficial in many aspects. First, a history may show the information about the ability of an entity. Second, history deters moral hazards in the present: each entity will perform to the best of its ability because current actions will become history in the future. Finally, since histories reveal information about a node's abilities, nodes with higher abilities are distinguished from the nodes having lower abilities. Reputation based systems usually collect, maintain, and disseminate reputation information in the network. In a MANET environment, reputation information is gathered either by

passive acknowledgments (promiscuous mode listening) or by active two-hop acknowledgments. Reputation values are stored for each node and may be shared as second hand information with other neighbours as well. Eventually nodes having high reputation get services whereas nodes having low reputation are isolated from the network. In the next section we present reputation based schemes developed for use in MANETs.

B. Passive Acknowledgment Based Schemes

In these schemes, monitoring is done by making use of passive acknowledgments and the networking hardware will be put in promiscuous mode. They may not work efficiently in the presence of ambiguous collisions, partial dropping, and unidirectional links.

Two techniques were proposed by Marti *et al.* [7]: Watchdog and Pathrater which run on the Dynamic Source Routing (DSR) protocol. Watchdog is a process running on each node that maintains a reputation table to record the reputation of one hop neighbours. Every time a source node *S* sends a packet to the destination node *D* via intermediate nodes, *S* holds a copy of the packet in memory until it overhears (in promiscuous mode) the same packet forwarded by the intermediate node before time *T* expires. The node *S* increases the reputation of the next node when it is confirmed that it has forwarded its packet, and decreases it otherwise after a time-out period. If the neighbouring node drops packets exceeding a given threshold the node is deemed to be misbehaving. Pathrater is used to evaluate paths in order to avoid the path having misbehaving nodes. Each node maintains a list of ratings for every neighbour node in the range from 0 to 1. Node ratings are initialized to a neutral value such as 0.5 and then incremented or decremented depending upon behaviour. Using these ratings Pathrater evaluates paths and selects the one having the highest rating. This technique has no punishment for misbehaving nodes, a drawback which is addressed by the CONFIDANT scheme.

Buchegger and LeBoudec [8] proposed an extension to DSR protocol called CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks), which is similar to Watchdog and Pathrater. It has four main components: the Monitor, the Trust Manager, the Reputation System, and the Path Manager. The Monitor applies similar techniques to those of the Watchdog process as it promiscuously listens to neighbours but also observes route protocol behaviour. The Trust Manager is responsible for sending an ALARM to all its friend nodes when misbehaviour is detected, and other trust managers receiving ALARM messages determine the trustworthiness of the message by scrutinizing the trust level of the sender. Based on this information the Reputation System maintains a local rating list and a blacklist, and further exchanges these lists with friends. Finally the Path Manager, which applies similar techniques to those of Pathrater, evaluates paths according to the reputation of nodes along the path and discards paths that

include misbehaving nodes. Since this protocol allows nodes in the network to send ALARM messages to each other, it could give more opportunities for attackers to send false alarm messages that a node is misbehaving while this isn't actually the case, a process referred to as rumour spreading [9]. The authors enhanced their scheme in Sonja and Buchegger [10] by using a Bayesian model that classifies and rules out liars.

As with the previous schemes, CORE [11] also relies on the DSR routing protocol. It also monitors neighbours via the watchdog mechanism. CORE combines three types of reputation information: subjective (direct) reputation, indirect reputation (but only positive reports are gathered to avoid blackmailing) and functional reputation. Functional reputation depends on certain functions which are given a weight based on their importance, for example control packets are considered less important than data packets, and hence more weight is given to data forwarding functions. These reputations are combined for a node to have an aggregate reputation in the network. Nodes having reputation below a given threshold are isolated from the network. An isolated node can, however, rejoin the MANET if it successfully increases its reputation by cooperating well for a period of time. To protect nodes suffering temporarily from bad environmental conditions, more weight is given to past behaviour. However this provides an opportunity for an attacker to misbehave after building up a good reputation.

C. Problems with Passive Acknowledgment

Most of the reputation based schemes make use of promiscuous listening or passive acknowledgments to observe their neighbours for packet forwarding activities. Apart from its advantages, such as the fact that it needs no specialized hardware ensuring low cost, it has several disadvantages which are caused by the peculiarities of mobile ad hoc networks. Marti *et al.* [7] identify the following weaknesses of the Watchdog mechanism in the presence of which it might not detect a selfish or misbehaving node.

Ambiguous collision: as shown in the scenario demonstrated in Figure 2, an ambiguous collision occurs at *A* while it is listening for *B* to forward a packet on. Node *A* does not know whether the collision is caused by its neighbouring nodes or by node *B*.

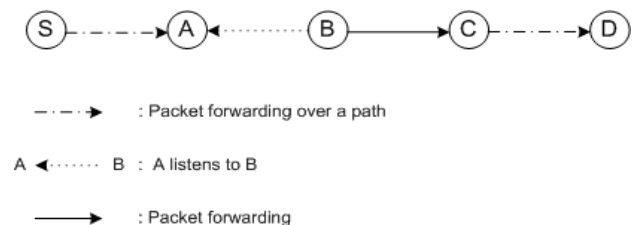


Figure 2: Passive Acknowledgment.

Receiver collision: due to the receiver collision problem node A can only tell whether B sends the packet to C , but it cannot tell whether C received it. Node C might not receive the packet because of a collision.

Limited transmission power: a node can limit its transmission power such that a signal is sufficiently strong to reach the previous node while weak enough not to reach the true recipient.

Collusion: more than one misbehaving node can collude to disrupt the Watchdog mechanism. For example, B forwards a packet to C but B does not report to A when C drops the packet.

Partial dropping: when a node drops packets at a rate lower than the configured misbehaving threshold.

D. Active Acknowledgment Based Schemes

These schemes do not suffer from the problems mentioned above, but instead of listening to passive acknowledgements, they explicitly send acknowledgements to inform the source node of packet receipt. For this, they incur extra overhead; however some schemes use Piggybacking to decrease the overhead incurred.

Kejun *et al.* [12] proposed a scheme that focused on the detection of misbehaving links instead of misbehaving nodes and which may be used as an add-on to the existing source routing protocols, such as DSR. The scheme makes use of a special acknowledgment packet which has been assigned a fixed route of two hops or three nodes in the opposite direction of the actual data traffic flow. Three consecutive nodes (triplets) N_1 , N_2 , and N_3 are assumed to lie along the path from source to destination. When N_1 forwards a packet to N_3 via N_2 , N_1 will not be sure whether N_3 received the packet due to the misbehaviour or ambiguous collisions in the path. In order to confirm the packet reception N_3 will send an ACK packet to N_1 via N_2 , called 2ACK. Among the triplet, N_1 is the observer (or ACK receiver) of the link $N_2 \Rightarrow N_3$. This triplet formation is carried out along the whole path.

For every outgoing packet N_1 will store the ID of the packet for time t in a list it maintains. When an ACK is received for a packet and matched to an ID in the list before time t expires, the entry in the list is discarded and a special counter C_{pkt} is incremented and C_{mis} is incremented otherwise. After a time period T_{obs} the ratio of C_{mis} and C_{pkt} is compared with a preset threshold R_{mis} , if the ratio is greater than the threshold all nodes are reported regarding the misbehaving link $N_2 \Rightarrow N_3$ by sending a RERR message. Each node receiving or overhearing such a RERR message deems $N_2 \Rightarrow N_3$ as a misbehaving link. These links are then avoided in the future. Nodes such as N_2 should not alter the 2ACK packet passing through them; a one-way hash chain mechanism is used as an authentication scheme to avoid such tampering.

Zhao *et al.* [13] proposed MARS (Misbehaviour Detection in Ad Hoc Networks), which provides protection against individual or cooperative misbehaving nodes. It does not need

any trust relationship or intrusion detection system for detecting misbehaviour. The scheme combines the multipath routing and single path data transmission with an end-to-end feedback mechanism. Before a source node starts communication with a destination node, it first selects two node-disjoint paths from its path list; one is used for data transmission and the other is for transmission information exchange. When the first data packet is sent on one path then a special control packet INF is sent through the other path to inform the destination about the data rate, packet size, and other path related information. The destination node then detects misbehaviour by analyzing the actual data received and the data sent by the source node. If the data rate falls below a certain threshold or the packets are tampered with then it notifies the source node about the misbehaviour along the path using a special control packet called an NTF. Authentication is used on source and destination nodes only. Upon receiving an NTF packet the source node will remove the paths from the list and select two other paths; otherwise it will start a new route discovery process.

MARS reduces the overhead as compared to 2ACK; however, because it only detects misbehaving *paths* it can reduce the chance of utilizing good nodes that happen to fall along a path with another node that misbehaves. There is no punishment strategy, so if the number of selfish nodes increases then there would eventually be no path available for data transmission.

Graffi *et al.* [14] propose a scheme which they call LeakDetector. It works on proactive routing and uses both the Watchdog mechanism and active acknowledgments for single or colluding nodes. Each source node maintains a traffic counter for each path indicating the amount of traffic transmitted to that path. T_{total} and T_i fields are maintained to track the overall traffic sent and the amount of traffic a node i forwards in relation to the total traffic respectively. Along the path, data will be passed through nodes. Let's say N_1 passes data to N_2 . Then N_2 will first append its information to the visited node list field in the packet and then reports the amount of data received from N_1 in the T_{N1} field in relation to the preset field T_{total} .

The destination node creates a virtual graph based on the information received (T_{total} and T_i) from the nodes constructing the path. Vertices represent nodes and edges represent the amount of traffic flowing between two nodes. The graph obviously exhibits the top level view of the whole traffic flowing in the path. When the destination node determines a node with significant in/out traffic flow variation, it is reported to the source node via a route reply message on a disjoint path. The source node can then take further action by updating the blacklist table or using a reputation technique to punish the malicious node. Moreover traffic counters are refreshed periodically to detect a node that was previously cooperating and then switched over to malicious behaviour.

TABLE 1: COMPARISON OF SCHEMES.

Scheme	Observation	Detection	Punishment Strategy	Features	Limitations
Watchdog [7]	Passive	Single Node	No	Path ranking based on selfish nodes in them; hence selfish nodes are bypassed.	Observation is based on passive ack.
CONFIDANT [8]	Passive	Single Node	Yes	Selfish nodes are isolated and trusted recommendations are taken into account.	Observation is based on passive ack.
CORE [11]	Passive	Single Node	Yes	Second chance is given for nodes in bad locations and no negative ratings are communicated.	Dependence on passive ack, more weight is given to past behaviour and hence recent misbehaviour will be ignored.
2ACK [12]	Active	Single Node	Yes	Use active acknowledgments for two hops to remedy the problems in promiscuous listening.	Substantial memory and message overhead.
MARS [13]	Active	Collusion	No	Acknowledgment from destination to source using node-disjoint multiple path.	Large memory overhead caused by storing multiple node-disjoint paths and sometimes it does not utilize good nodes because it deletes paths containing selfish nodes.
LeakDetector [14]	Both	Collusion	Yes	Destination node creates a virtual graph of the traffic it receives from a source, and hence it helps to identify traffic leaks.	Large memory overhead and evaluation is based on limited nodes with no mobility.

Graffi *et al.* have evaluated the scheme on seven stationary nodes. Since it is proposed for use in MANETs, an increased number of nodes in a mobile environment are needed for a more complete evaluation.

III. DISCUSSION AND FUTURE DIRECTIONS

Table 1 summarizes the important features and limitations of the schemes we discussed in Section 2 of this document. Generally speaking, passive acknowledgment techniques are more promising than active acknowledgment techniques because they do not cause any extra communication or memory overhead. Active acknowledgment provides reliability at the cost of extra memory and communication overhead but in the environments where there is a high collision rate it is as prone to errors as promiscuous listening techniques. Schemes using node-disjoint multipath routing maintain a large cache for storing these paths. Since in mobile environments path reconstruction rate can be high, this may cause substantial overhead and delay due to the frequent path discovery messages in the network. Furthermore, acknowledgments no matter if explicit, may still be lost due to high mobility or collisions resulting in further overhead in the form of retransmissions. On the other hand coping with high mobility situations can be handled in mobile ad hoc networks while using promiscuous listening techniques only by relaxing the misbehaving threshold. Buchegger *et al.* [15] conducted a test-bed to establish how efficient promiscuous listening is and they discovered some very interesting results. First, in high traffic loads they did not experience a single collision; hence there was a very low chance of ambiguous and receiver collisions;

however these can still be compensated by adjusting the threshold. Second, they found out that it is not easy for a misbehaving node to drop a packet due to malicious power adjustment (limited transmission power) because it is difficult to achieve power range adaptation using current off-the-shelf hardware. Third, in some situations passive acknowledgments perform even better than active acknowledgments.

The main purpose of any cooperation enforcement scheme is to detect and isolate misbehaving nodes. In other words, any node must face the consequences of its actions. However, this accountability is based on identity (implying a network entity), which can be easily obtained, changed or discarded in mobile ad hoc networks given that there is no centralized identity management. As there is no restriction on identity creation a user can create as many identities as he/she wishes. Consequently, a node having poor reputation or trust background discards its identity and whitewashes its previous misbehaving history and starts afresh. This is called Whitewashing. There is a potential need to develop lightweight techniques, such as non monetary fee per identity, to maintain identity persistence in the network and to discourage whitewashers; otherwise it is of no use to build up trust or reputation. By non monetary fee we mean some work done in terms of cooperation per identity in the network.

Finally, Sybil attacks [2] are a serious threat to the above mentioned schemes, where a malicious node can generate and control a large number of logical identities on a single physical device. This gives the illusion to the network of it being various different legitimate nodes. A Sybil attacker can increase its reputation or trust value and can also decrease the same value for the other legitimate nodes by exploiting its

virtual identities. Identity distinction and persistence must therefore be taken into account when designing such schemes because accountability is their sole purpose. A possible distributed solution to detect Sybil attacks might be the use of low cost localization, where each identity will be bounded by a single physical location at any particular time. A node can easily detect Sybil attack when receiving from multiple identities transmitting from same location. Signal strength based localization techniques [16-18] are promising because they require no extra hardware for localization.

IV. CONCLUSION

Selfish or misbehaving nodes degrade overall system performance and pose a serious threat to multihop routing in MANETs. Reputation based models play an important role in detecting and isolating selfish nodes. In this paper we categorized reputation based schemes based on monitoring approaches: active and passive based acknowledgments. Finally, we discussed their pros and cons as well as some other important identity related issues and suggested some directions for future work.

REFERENCES

- [1] J. Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Computing Surveys*, vol. 39, p. 1, 2007.
- [2] J. R. Douceur, "The Sybil Attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*: Springer-Verlag, 2002.
- [3] D. P. Agrawal, , and Q. A. Zeng, "Chapter 13, Ad hoc and Sensor Networks," in *Introduction to Wireless and Mobile Systems*: Brooks/Cole-Thomson Learning, 2003, pp. 297-348.
- [4] Y. Yoo, S. Ahn, and D. P. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in *IEEE International Conference on Communications (ICC)*. vol. 5, 2005, pp. 3005-3009
- [5] L. Butty and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Network and Applications*, vol. 8, pp. 579-592, 2003.
- [6] E. Friedman, P. Resnick, and R. Sami, "Ch: 27- Manipulation-Resistant Reputation Systems," in *Algorithmic Game Theory*, N. Nisan, V. V. Vazirani, E. Tardos, and T. Roughgarden, Eds. New York: Cambridge University Press, 2007, pp. 677-697.
- [7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking* Boston, Massachusetts, United States: ACM, 2000.
- [8] S. Buchegger, J. Yves, and L. Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* Lausanne, Switzerland: ACM, 2002.
- [9] S. Buchegger, L. Boudec, , and Jean-Yves, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks," in *Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, France, 2003.
- [10] Sonja and Buchegger, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proceedings of P2PEcon*, Harvard University, USA, 2004.
- [11] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*: Kluwer, B.V., 2002.
- [12] L. Kejun, D. Jing, K. V. Pramod, and B. Kashyap, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, pp. 488-502, 2007.
- [13] L. Zhao and J. G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks," in *IEEE Global Telecommunications Conference (GLOBECOM) 2007*, pp. 941-945.
- [14] K. Graffi, P. S. Mogre, M. Hollick, and R. Steinmetz, "Detection of Colluding Misbehaving Nodes in Mobile Ad Hoc and Wireless Mesh Networks," in *IEEE Global Telecommunications Conference (GLOBECOM) 2007*, pp. 5097-5101.
- [15] S. Buchegger, C. Tissieres, and J.-Y. L. Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks " How Much Can Watchdogs Really Do?," in *Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications*: IEEE Computer Society, 2004.
- [16] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks* Los Angeles, CA, USA: ACM, 2006.
- [17] S. Abbas, M. Merabti, , and D. Llewellyn-Jones, "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks," in *Second International Conference on Developments in eSystems Engineering (DESE)*, 2009 2009, pp. 190-195.
- [18] M. S. Bouassida, G. Guette, M. Shawky, and a. B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET " *International Journal of Network Security*, vol. 8, pp. 322-333, May 2009.