International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Survey on Reputation and Trust in MANETS

A. S. Gowri
AP/CSE, Dr. Pauls Engineering College,
Pauls Nagar, Pulichapallam, Vanur, Villupuram Dt., Tamilnadu, India
Email: sivakgowri@gmail.com

***Abstract* – Wireless Self organizing networks rely[1] on node cooperation to perform and support basic functions like packet forwarding, routing and network management . Lack of Infrastructure, resource constraints and organizational environment of self organizing nodes make them vulnerable to newer threats and challenges. By default, [2] non-cooperative misbehavior activities of the nodes will slowly lead to the performance deterioration of the network. Hence the responsibility of ensuring security and Integrity is its vital role of these self organizing networks. Cooperation enforcement schemes [3] like reputation and trust provides a supplementary security to protect basic network operations from misbehavior threats of the internal nodes.**

***Keywords* – Cooperation Enforcement, Reputation, Trust, Misbehavior, Network Functions.**

I. INTRODUCTION

Distributed Collaborations and Information sharing are considered to be the essential operations in wireless self organizing Networks. [4] The wireless self organizing networks like Manets, P2P, WSN have undergone tremendous technological advances over the last few years. This rapid development has also led to newer threats & challenges of ensuring security over these networks. Autonomy of nodes, [3] lack of centralized infrastructure, resource constraints makes the nodes vulnerable to selfish and malicious behavior. Traditional Network Security deals with the cryptographic mechanisms that ensures integrity, authentication and confidentiality aspects of a system. [5] However, cryptographic security is not sufficient for defending against the misbehavior resulting from selfish and malicious nodes in the network. [1] These problems can be solved by incorporating reputation and trust systems in wireless self organizing networks.. This not only provides the capability of informed decision making but also provides them with security against any internal attacks which cannot be addressed by conventional security system.

A Manet is a self configuring system of mobile nodes connected by wireless links. The nodes are free to move randomly, changing the networks topology rapidly and unpredictably. [7] Manets are highly preferred for connecting mobile devices quickly and spontaneously in emergency situation like rescue operation, disaster relief, military operations. Manets are decentralized where nodes are autonomous and do not have any common goal. The intermediate nodes on a communication path are expected to forward packets of other nodes so that the mobile nodes can communicate beyond their wireless transmission range. The transmission range is limited due to the power constraint and there is no fixed communication infrastructure to facilitate packet forwarding. It is advantageous for individual nodes not to cooperate with the network. [2] The Non-Cooperative behavior could be selfish or malicious. The non-cooperative nodes may be unwilling to spend its resources in performing network functions which are not of its direct interest, even though it expects other nodes to forward its packets to the destination. Such non-cooperative nodes degrades the overall performance of the network.

The rest of the paper is organized as follows. Section II presents the literature of reputation and trust schemes along with their pros and cons. The Annexure I discusses a comparative statement about the schemes under various parameters. Section III introduces the areas which these schemes gives way and finally section IV concludes this survey highlighting future plans.

II. LITERATURE REVIEW

A. CORE

A Collatborative Reputation mechanism to enforce node cooperation in Manets [15] is proposed by Michadi and Molva in 2002. It is a distributed symmetric reputation model. The CORE acts as a layer on the top of the DSR protocol and uses bidirectional communication symmetry. CORE also assumes promiscuous mode operation. [13] Each node in CORE maintains a Reputation Table RT one for each specific function like route discovery, packet forwarding etc.. The reputation is calculated based on 3 types namely subjective, Indirect and Functional reputation.

The subjective reputation is computed giving more weight to the past observation also termed as first hand reputation. The negative observation is assigned a rating of -1 and +1 to positive observation. The value 0 is assigned either for neutral observation or for the new entry of a node. These rating factor contributes to the computation of reputation. The indirect reputation deals with the recommendations from other nodes otherwise termed as second hand information. The functional reputation is computed for each specific function is based on the combination of subjective and indirect reputation with appropriate weights assigned to each. The subjective reputation is calculated during the request phase and updated by watchdog mechanism whereas the indirect reputation is during the reply phase that contains the list of nodes that correctly behaved in context of each function.

CORE dessiminates [11] only positive rating thereby avoiding BMA on benign nodes. Though CORE do not excludes selfish nodes on [14] sporadic misbehavior, it does not provide second chance mechanism to malicious node. It promotes false praise attack thereby encouraging colluding malicious nodes to survive for a longer time.

Inference:

Avoiding second chance mechanism eliminates unnecessary risks. The classified Reputation computations reduces complexity and made understandable but also leads to considerable overhead. Retention of selfish nodes and getting them activated saves node density thereby maintaining network performance. Using both the first hand and second hand information but weighing the former high makes the system believe its own observation than recommendations.

B. CONFIDANT :

Cooperation of Nodes Fairness in Dynamic Adhoc Networks[12] is proposed by Buchegger and Bondec in 2002. It is also a distributed symmetric reputation scheme that uses DSR routing protocol and assumes promiscuous mode of operation. Unlike other reputation system CONFIDANT classifies the first hand Information as Personal experience and Direct Observation, where the second hand information is termed as recommendation based. Each node consists of four components – the Monitor, Trust Manager , Reputation system and Path Manager.

The Monitor detects the deviations of the next node on the source route by either listening the transmission or by observing route protocol behavior. It sends an alarm to the trust manager to indicate a bad behavior. The Trust manager handles the alarm table, trust table and friends list. The alarm table contains information about received alarms. The trust table stores the trust values of nodes to determine trustworthiness. The friend list contains details about nodes to which alarm has to be sent to inform about malicious nodes, The trust manager takes decision about providing or accepting routing information, accepting a node as a part of a route, taking part in a route originated by some other node.

The Reptuation System maintains a table that consists of entries of other nodes and their corresponding reputation values. The reputation rating of a node is updated only when the sufficient evidence of malicious behavior of that node occurring atleast for a threshold number of times. Higher weight is given to personal experience than observation. The Path Manager reranks the path according to the reputation value of the nodes in the path, delete path containing malicious nodes, decides whether to ignore a request from a malicious node or alert the source for a route containing malicious nodes.

CONFIDANT exchanges only negative rating between nodes, [11] the system is vulnerable to False Accusation of benign nodes. CONFIDANT do not discriminate between selfish and malicious nodes. With negative rating beyond threshold, misbehavior nodes are excluded and recovered after a timeout.

Inference:

CONFIDANT reputation system addresses a number of performance metrics. Unbiased treatment to selfish and malicious nodes will result in lose of node density, thereby affecting the performance of critical networking functions. Dissemination of negative rating leads to False Accusation Attack of benign nodes. Re-entry of excluded nodes costs additional overhead with risk. Each Node equipped with too many components pulls back the resource efficiency. Though Second Hand Information considered for reputation first hand information is weighed more.

C. OCEAN :

Observation Based Cooperation Enforcement in Adhoc Networks [9] has been proposed by Bansal and Baker as a security layer over the DSR protocol. The Objective of OCEAN lies in maintaining the overall packet throughput of an adhoc network in the face of nodes that misbehave at the routing layer. It focuses on the robustness of packet forwarding on the routing layer and do not address attacks at lower layers. OCEAN addresses on orthogonal issues encouraging routing participation and responds complete threat model.

The OCEAN layer that resides on each node hosts five components. The Neighbor watch purely monitors the behavior of neighbor node. It registers either positive or negative events depending upon if a packet is forwarded or not. These events are communicated to RouteRanker which maintains ratings of the neighbor node. The rating is initialized to neutral and is incremented or decremented on receiving positive or negative events from Neighbor watch component. The Rank based Routing module avoids routes containing nodes in the faulty list. [4] The Malicious traffic rejection module rejects the traffic from nodes it considers as misleading. The Second chance mechanism module gives opportunity to the faulty nodes to demonstrate the goodness by removing it from faulty list after a timeout. Even then its rating is not increased to neutral so that it can be quickly added back in the faulty list in the event of continuous misbehavior. The selfish nodes are treated on trade based schemes. Every node maintains chip count for each neighbor. Chip Accumulation Rate is the rate at which all chip counts in the network are increased per unit time. [6] A node earns a chip upon forwarding a packet and loses a chip when asks to forward a packet. A low CAR value punishes selfish nodes.

Inference:

Nodes rely on their own observations thus avoiding the vulnerabilities arising out of second chance mechanism. Hence a considerable overhead of computing second hand reputation is reduced. OCEAN is less complex and less vulnerable to BMA as it disallows second hand reputation exchanges. This leads to simplicity of mitigating selfish node reduces complexity. OCEAN shows far better throughput performance compared to schemes that share second hand reputation. Rejoining the faulty nodes as they start behaving better is an excess overhead with uncertainty. At the same context, the bootstrap to compute the reputation of nods takes more time as the system depends only on its own observation. The Overhead in maintenance of chip count and Trade off required for setting up appropriate Chip Accumulation Rate.

D. SORI:

SORI [8] In Secure and Objective Reputation based Incentive Scheme for Adhoc Networks the transmission range of a mobile node is limited due to the power constraint and there is no fixed communication infrastructure to facilitate packet forwarding. Hence the

communication between two nodes beyond the transmission range solely depends on intermediate nodes to forward packets. Hence the continuous cooperation of the intermediate node is mandatory for the success of an adhoc network. SORI encourages packet forwarding and penalize selfish nodes. SORI addresses on three issues of selfish nodes. First, Reputation of a node is quantified by objective measures, secondly Propagation of reputation is secured by a one way hash chain based authentication scheme. Last, the reputation of a node propagated only to neighbours thereby reducing communication overhead.

SORI falls into the category of reputation based incentive schemes [14] for packet forwarding which consist of neighbor monitoring, reputation propagation and punishment. Neighbour monitoring collects information about misbehavior of neighbor nodes and objectively quantifiying reputation of neighbours. The reputation is determined by the ratio of the number of forwarded and observed to the number of packets that a node is requested to forward. [15] Reputation Propagation is aimed at sharing information among neighbouring nodes. Punishment is to encourage packet forward and discipline selfish nodes. SORI can successfully identify selfish nodes and punish them.

Inference:

Communication overhead is reduced considerably by propagation of reputation only to the neighbor nodes. SORI addresses issues only on selfish behavior of nodes. The Objective Quantification of reputation is limited to the probability of transmission collision as the reputation ratio is not reflected due to packet collision in wireless medium. The overall comparison of the four types of reputation system is shown in the table attached as annexure. The reputation schemes are compared under various network dynamics that leads to the requirement of a unified framework.

III. Discussion

After surveying the schemes presented here it is found that there are issues that can be addressed better. The schemes represents critical networking functions like packet forwarding and routing functions. The simulations focus on throughput, packet loss and delay. Each scheme is based on different assumptions while the trust and reputation framework considered varies significantly. Measure can be taken to find how to stimulate the selfish nodes to announce true residual battery energy. The Reputation schemes can be analysed for different node mobility and node density. The trust systems that uses first hand information alone faces BootStrapping problem in identifying the malicious nodes. Further the relationship between network dynamics and trust dynamics are yet to be analyzed. The issues of trust computing mechanisms like distributed trust or centralized trust can also be focused.

IV. Conclusion & Future Plan

With the literature survey schemes available it is found that the different approach lacks unity for comparison. Each scheme is based on different assumption while trust and reputation framework considered varies significantly in many aspects. The presented schemes addresses issues like information gathering, propagation, consideration of first and second hand information, identification of misbehaving nodes, action taken, node reintegration in the system. A strong cooperation enforcement mechanism that is resource efficient with minimized overhead in manets is needed. The future work will continue in that direction with a unified framework. Though the simulation results are provided, it cannot be concluded as optimal solution as the simulation configurations, parameters, assumptions made vary significantly.

This paper presented a literature survey on reputation based system to enforce cooperation in manets with their distinctive features with relative merits and demerits. The paper recognizes the special requirements of manets in terms of cooperation, robustness, fairness against spurious ratings under a common reference scenario.

References

[1] Avilash Samantara " Reputaion & Trust based Systems for wireless Self organizing networks" – A Technical Seminar Report, March 2013.

[2] S. Kami Makki, Lamar University, Beaumont, Texas, USA Keenan B. Bonds, Norfolk State University, Norfolk, Virginia, USA. Enhancing Node Cooperation in Mobile Ad Hoc Network JOURNAL OF NETWORKS, VOL. 8, NO. 3, MARCH 2013.

[3] Atul Kumar Purohit Bhopal Mukesh Kumar Baghel Hitesh Gupta Comprehensive Analysis of Cooperation and Misbehavior Issues in Ad hoc Wireless Networks Council for Innovative Research International Journal of Computers & Distributed Systems www.cirworld.com Volume 1, Issue 2, August, 2012.

[4] A. Jangra1, Goel, Priyanka N. and, K. Bhati, Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189-196, 2010.

[5] Kannan Govindan and Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks : A Survey" in IEEE Global Communication Conference, Globecom 2010.

[6] Jaydipsen "A Survey on reputation and trust based systems for wireless communication networks, 2008.

[7] G. F. Marias1*,y, P. Georgiadis1, D. Flitzanis2 and K. Mandalas2, Cooperation enforcement schemes for MANETs: A survey, Wireless Commun. Mob. Comput. 2006;WIRELESS COMMUNICATIONS AND MOBILE COMPUTING 6:319–332 Published online in Wiley InterScience (www.interscience. wiley.com). DOI: 10.1002/wcm.398.

[8] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks," Proceedings of WCNC 2004, Atlanta, GA, March 2004.

[9] Sorav Bansal and Mary Baker, Observation based cooperation enforcement in ad hoc networks" Technical Report, Stanford University, arXiv:cs.NI/0307012 v2 6 Jul (2003).

[10] S. Buchegger and Jean-Yves Le Boudec. Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad Hoc Networks. EPFL Technical Report Number IC/2003/31, 2003.

[11] S. Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol; Cooperation of Nodes -Fairness in Dynamic Ad Hoc NeTworks. In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002.

[12] L. Buttyan and J. Hubaux. Stimulating Co-Operation in Self Organizing Mobile Ad Hoc Networks. Technical Report DSC/2001/046, EPFL-DI-ICA, August 2002.

[13] Pietro Michiardi and Re_k Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks.

International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Annexure I: A Comparative Statement about the Reputation and Trust Schemes under various Parameters

S.No	Reputation and Trust Scheme	Author & year	Reputation / Incentive based	First Hand Info Rating.		Second Hand Information for rating	Exclusion of selfish / malicious nodes	Second Chance Mechanism
				Personal Experience rating	Direct Observation rating			
1	CORE	Michadi & Molva, 2002	Reputation	Not exist	More weight (subjective reputation)	Less weight (Indirect reputation)	Only malicious node excluded	No
2	CONFIDANT	Buchegger & Bondec, 2002	Reputation	More weight		Less weight	Both	Yes, after a timeout.
3	OCEAN	Bansal & Baker, 2003	Reputation and Incentive	Not exist	Considered	Not Considered	Both	Yes, after a faulty timeout
4	SORI	Qi HE, Dapeng Wu, 2004	Incentive based	Neighbor monitoring (objective reputation)		Not Considered	Selfish Nodes	Yes

S.No.	Reputation and Trust Scheme	Information Dissemination	Mathematical model used for reputation computation	Simulation Observation based on	Means of Performance analysis	Performance metrics considered
1	CORE	Positive	Weighted Mean	Selfish Nodes	Berleley's Network Simulator NS-2	Throughput & Comm
2	CONFIDANT	Negative	Bayesian Statistics	Malicious Nodes	GloMoSim for MANETS	Throughput, Good put, Packets dropped
3	OCEAN	Positive	Statistical	Misleading & Selfish Nodes	GloMoSim	Packet Throughput
4	SORI	Positive	Weighted Averaging	Selfish Nodes	NS-2	Packet throughput