Survey of Trust Schemes on Ad-Hoc Network

Renu Dalal[1,*], Manju Khari[1], and Yudhvir Singh[2]

[1] Computer Science & Engg.Department, Ambedkar Institute of Technology, New Delhi, India
[2] Department of Computer Science & Engg, U.I.E.T M.D University Rohtak, India
dalalrenu1987@gmail.com

Abstract. MANET (Mobile Ad-hoc Network) is a structureless & dynamics network, which consist of mobile nodes without any physical link between them. MANET provides some basic functions like routing, communication, network management and packet forwarding etc over self organized network. Because MANET has not a fixed topology, in which mobile nodes comes and leaves the network within a random period of time. It effects energy, bandwidth and memory computations of network. Providing trust in MANET is such a crucial task because it doesn't having centralized infrastructure. In this paper, we survey the different trust model schemes of MANET with their unique features, merits and demerits.

Keywords: MANET, Cluster based, Maturity based, PKI, ABED, CORE.

1 Introduction

Security is an important issue in wired network (like LAN, WAN, Ethernet etc) as well as in wireless network (wireless sensor network, cognitive radio network, MANET etc).Trust models are necessary to provide security in networks. In MANET trust can be defined as a level of belief according to the behavior of nodes (or entities, agents etc) [1].The probability value of trust varying from 0 to1, where 0 represent DISTRUST and 1 represents TRUST [2]. According to Golybeck [3] trust has three basic properties: Transitivity, Asymmetry and Personalization (or personal opinion).

The different existing trust based schemes in Ad-hoc network were discussed in this paper as shown in fig. 1. *Section 2* Including Protocol based trust schemes (ABED, GRE, OTHER). *Section 3* presents seven different System level based trust models, *Section 4* will give the review of Cluster based trust model, *section 5* covers Maturity based trust model. PKI based trust model comes in *section 6* and conclusion in *section 7*.

* Corresponding author.

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 170–180, 2012.

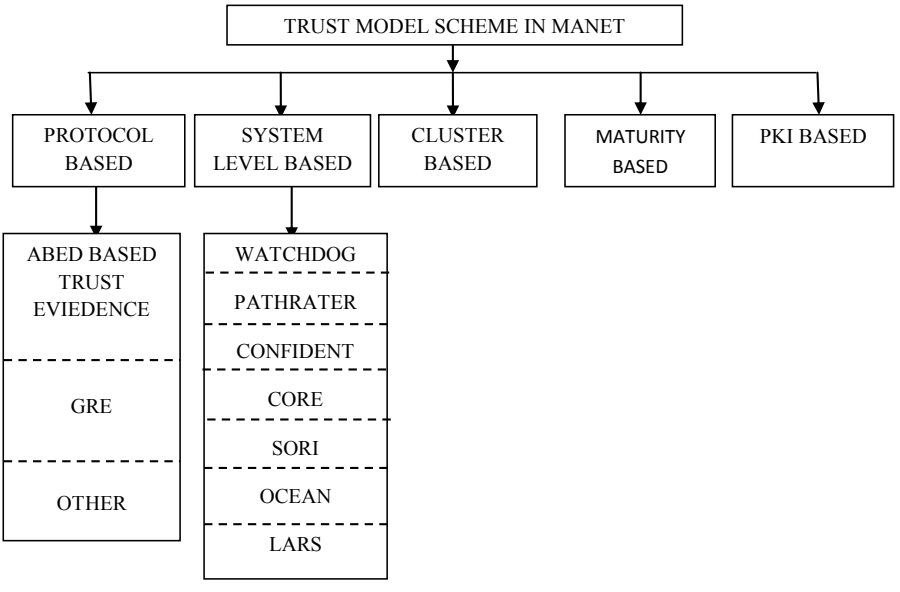


Fig. 1. Trust Based Schemes in MANET

2 Protocol Based Trust Schemes

2.1 ABED

ABED is Ant Based Evidence Distribution scheme, which was purposed by Jiang & Baras [4]. This scheme uses the concept of swarm intelligence paradigm. In this scheme, mobile nodes (in MANET) communicate indirectly with other mobile nodes through "agents" which called "ants" in ABED. Agents found the optimal path for evaluating trust evidence, through the information called "Pheromones" that is collected by "ants". Features of ABED: Easily adaptive to mobility, effectively work in structure less network. It can solve the problem of Dynamic optimization and combinatorial optimization. Work on Stigmergy principle.

2.2 GRE

Generalized Reputation Evidence (GRE) protocol based scheme is discovered by Buckerche & Ren [5]. The main feature of GRE is, it provide security to trusted community of MANET from malicious nodes because GRE scheme will not entered any suspicious node in trusted network. Merit of this scheme, neither attack is addressed on GRE model.

2.3 Other Scheme

Trust evidence evaluation scheme is discovered by Theodorakopoulos and Baras [4]. Features: Solving path problem in directed graph. Theory of Semirings is used for

provide trust between nodes (where node as entities and link between two nodes as trust relationship) without using direct communication between them. This model is robust in nature in presence of Intruders. Binary variables (0 or 1) used as trust value. Trust is transistive according to this model.

3 System Level Based Trust Models

System level trust model is the combination of Individual level trust model and punishment or reward system. In this model, system will give punishment to those nodes which found as malicious or selfish in network and also give reward to those nodes which behave in a trustworthy way most of the time. The system level trust model includes "Trust evidence dissemination mechanism" [6].

3.1 Watchdog

In 2000, the Watchdog trust model was discovered by [7]. Watchdog mechanism find out the selfish node in MANET by observing each and every function (listening next node's transmission, exploiting promiscuous mode of operation etc) performed by mobile node. The mobile node considered as malicious node in the two cases and source is notified, *case 1*: if the packet is not forwarded by node within a certain period of time in network. *Case 2*: each node have a buffer for keeping recently sent packets, if overheard packet is not same as one stored in buffer.

3.2 Pathrater

Pathrater behaves as the Watchdog with including the feature of providing the" best route link (which is likely to be reliable) [7] for reliable data". For searching the best route for data, node calculates the path metric according to observe the rating for every neighboring node which is known in MANET. This scheme provides the shortest path selection when reliable information is not available. If negative value exists in path metric, it indicates one or more malicious node in the path.

3.3 CONFIDENT

CONFIDENT is a system level based trust model, which purposed in 2002 by [8]. Nodes are extracted in this model which does not behave normally in network. Implementation of Cooperation of Nodes Fairness in Dynamic Network (CONFIDENT) required four components: 1 Monitor:-The node found abnormal behavior by monitoring the transmission of next node or by behavior of route protocol. 2 Reputation System: - If any node found suspicious node in MANET, an ALARM message sent to the trust manager component. 3 Trust Manager: - It evaluates the trust of malicious node. The malicious node refers to as trustworthy node, if trust manager is not capable to prove malicious behavior (exceeding threshold to rule out coincidences etc). 4 Path Manager: - Each node having a list that contains the all malicious node and this list is interchanged at random period of time between other nodes.

3.4 CORE

Collaborative Reputation (CORE) trust scheme was founded in 2002 by [9]. CORE scheme differentiate the selfish node and malicious node. The nodes which not cooperate with other nodes in the MANET, for saving battery for its own communication is called "selfish node" while these nodes does not damage other node. The malicious node in MANET behaves abnormally and can damage other nodes by doing any suspicious activity. CORE purposed three different type of reputation: 1. Subjective Reputation: - Reputation value evaluated by giving priority to past observation of mobile node, rather than current one. If malicious node is found out then node's subjective reputation value is changed by using WD (watchdog) mechanism. 2. Indirect Reputation: - This value is calculated by providing reputation by one node to other node. Reputation value can be updated through reply message that contains the list of nodes which behaved normally in context of every function. If any node having negative reputation value all requested by that node will be rejected and this node works only as service provider not as requester. For long period of time if this node will provide correct services to all other nodes in MANET, node can achieved their reputation value again. When reputation value is above then the threshold reputation value, that node will again works as service provider as well as service requester. 3. Functional Reputation: - This reputation is the combination of indirect and subjective reputation value. The weight combine formula is used for calculation of functional reputation value.

3.5 OCEAN

Observation Based Cooperation Enforcement in Ad-hoc Network (OCEAN) trust scheme was discovered in 2003 by [10]. This scheme is not allowed to exchange the second hand knowledge about nodes to other nodes in MANET. OCEAN model has five components, 1. Neighbor Watch: - It will watch the behavior of neighboring node. 2 Route Ranker: - It maintains the route rank list for each of the neighboring node. 3 Rank based routing: - This component extracts those routes which contains malicious node. 4 Malicious Traffic Rejection: - All suspicious traffic is removed from node which consider as misleading by this component. 5 Second-chance Mechanism: - Malicious node is removed from the faulty list after a fixed duration of observation inactivity and constant value assigned to the node.

3.6 SORI

In 2004, Secure and Objective Reputation-based Incentive (SORI) scheme was discovered by [11]. SORI scheme takes concept of reputation rating which based on packet forwarding ratio of a node. It consists of three components, 1. Neighbors Monitoring, This component used to collect information of neighboring node about the behavior of packet forwarding. 2. Reputation Propagation: - It providing information sharing of other nodes with its neighbor. 3. Punishment: - It includes the process of removing the packet from the network. This scheme can't differentiate between the selfish and malicious node.

3.7 LARS

Locally Aware Reputation System (LARS) level trust model was purposed by [12] in 2006. It provides reputation value to its entire one hop neighboring node. This value can be changed on direct observation of neighbor node. The Warning message will be generated by the evaluator node (EN) to its neighbor, if EN founds any node's reputation value below to the threshold trustworthy value.

4 Cluster Based Trust Model

The cluster based trust model for MANET was introduced in 2008 by [13]. In this model, ad-hoc network divided into clusters. Important terms used in this model, 1. Direct trust value: - any two nodes in cluster calculate trust value between them according to recent transaction records. For ex.n2 and n3 takes α1 value as direct trust value in cluster c1. 2. Inter cluster trust value: - Cluster head collected the recommendation information from other nodes to compute the inter cluster trust value.3. Gateway: - It maintains interaction between MANET's node with adjacent cluster. 4. Routing:-Two type of cluster routing is used in this model. One is Intra-cluster routing, the routing with in a cluster. Another is Inter-cluster routing, the routing between two different clusters. Zone routing protocol is used in cluster based model, which is combination of "Proactive" (intra-cluster routing) and "Reactive" (inter-cluster routing).

(A) Direct trust Representation & Its Computation [13, 14, 15]
From Node N_J to N_i direct trust represented as TR^{ij}_D calculation of direct trust:

$$TR^{ij}_D = \frac{t_m + a/2}{t + a} \quad t_m,\ t \geq 0,\ a > 0 \tag{1}$$

In case, when there is no previous interaction between mode N_J and N_i.

t is the time transactions, t_m is time success and a is a positive real number. a is inversely proportional to evidence in this model.

(B) Intercluster Recommendation Trust Value's Representation & Its Calculation
It is denoted as TR^{j}_{r} and calculated as:

$$TR^{j}_{r} = \frac{\sum_{i=1}^{t} TR^{hi}_{D}.TR^{ij}_{D}}{\sum_{i=1}^{t} TR^{hi}_{D}} \qquad \text{Where } TR^{hi}{}_{D} > H,\ i \neq j. \tag{2}$$

TR^{hi}_D is aggregation weight (direct trust value of node N_i, computed by CH), TR^{ij}_D is direct trust recommendations information and n is the number of nodes in current cluster.

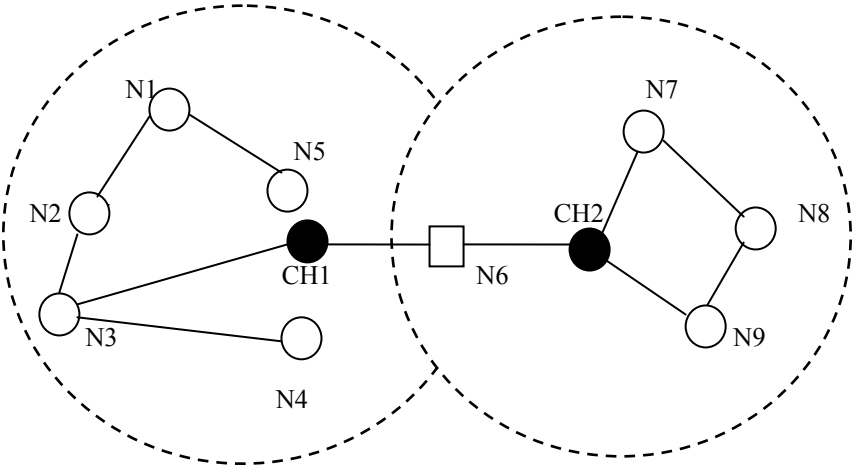
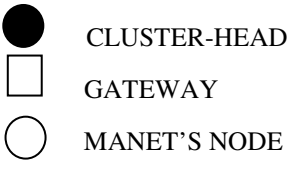


Fig. 2. Cluster Based Trust Model in MANET



(C) Total trust representation & computation

It is represented as $\Gamma(N_i, N_j)$ and computed as:

$$\Gamma(N_i, N_j) = \alpha\, TR^{ij}{}_D + \beta TR^{i}{}_r \tag{3}$$

Where $\alpha, \beta \geq 0$ and $\alpha + \beta = 1$. $TR^{ij}{}_D$ is the direct trust between nodes N_i and N_j, α is the impact weight of direct trust and β is the impact weight of recommendation trust.

(D) Cross cluster trust

The cross cluster trust between nodes N3 & N7 can be calculated as:

$$\Gamma(N3, N7) = \Gamma(N3, N6).\ \Gamma(N6, N7) \tag{4}$$

N3 node is in cluster c1 and N7 is in c2, through node N6 (gateway) both nodes are connected. Γ(N3, N6) is the global trust of node N6 by node N3.This trust value is calculated in c1 because node N3 and N6 locates in c1. Γ(N6, N7) is global trust, which calculates in cluster c2 because node N6 and N7 comes in cluster c2. Merits of cluster based trust model: No need of personal or past experience of any node in MANET for evaluation of trust value on nodes. Effective work in a small scale Ad-hoc network. Cluster head (CH) and gateways used in this model. There is no need of centralized infrastructure. Demerits: The performances will be degraded when cluster based model used in larger size MANET.

5 Maturity Based Trust Model

It was disclosed in 2010 by [16], figure [4] shows Maturity based trust model. Its features are as follows: This trust model introduces the concept of relationship maturity in Ad-hoc network. Trust increases between people as times goes by, same concept is used in maturity based model for MANET. Every node takes direct recommendation value to its neighborhood node only. This value will be decreased if new neighbor comes in network. This model purposed the REP (recommendation exchange protocol) for interchanging recommendation value for their neighbors.

(A) Calculation of recommendation value in Ad-Hoc

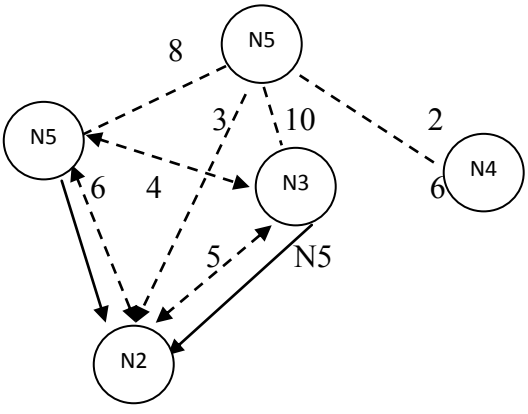


Fig. 3. Evaluation of recommendation value

In fig. [3], Decimal digits show how long the nodes know each other. Dotted arrows are used for connecting the neighboring nodes. Normal arrow indicates recommendation. Here N5 is neighboring node of N2, N1 & N3. Nodes N1 and N3 send recommendation value of N5 to N2. N2 consider the recommendation value (5) of N3 more important than N1 because node N3 knows node N5 as longer period of time also N3 having more older experience to interact with N5 as compared to N1.

(B) Maturity Based Trust Model Operation Modes

This model defines three types of operation modes. These are as follows: (i) Simple Mode, in which node using trust table and REP protocol optional. Nodes operated in less power capacity. (ii) In Intermediate Mode, nodes are operated in medium capacity and takes recommendations of other nodes. (iii)Advanced Mode, nodes are operated in higher power capacity & developed the system with all features. REP protocol is used for providing interface between network (TCP/IP) and trust, learning plan of System.

(C) Evaluation of Trust in Maturity Based Model

The evaluation of trust from node a to b is denoted as Ta (b). It takes the concept of T a (b) evaluation from [1]. Ta (b) = (1-α) Q_a (b) + α R_a (b); α ranges from 0 to 1, parameter in this model, that permits node to take most relevant factor. Q_a(b) lies

from 0 to 1 and presents direct value of node a to b. $R_a(b)$ lies between 0 to 1 and represents aggregate recommendation value of all other neighbors.

$Q_a(b) = \beta E_a(b) + (1-\beta) T_a(b)$; β lies between 0 to 1 and presents different weights for the factor of eq. & select best relevant at instance. $E_a(b)$ evaluates trust value by classifier components and $T_a(b)$ is the last trust value stored in trust table.

$$R_a = \frac{\sum_{i \in K_a} T_a(i) M_i(b) X_i(b)}{\sum_{j \in K_a} X_i T_a(j) M_j(b)} \tag{5}$$

Where $X_i(b)$ according to [18].

$X_i(b) = N(T_i(b), \sigma_i(b))$; $R_a(b)$ defined as recommendation value from all nodes, $i \epsilon K_a$ about node b, X(i) is the accuracy, M(i)is the relationship maturity and value in a trust table of node i to b.

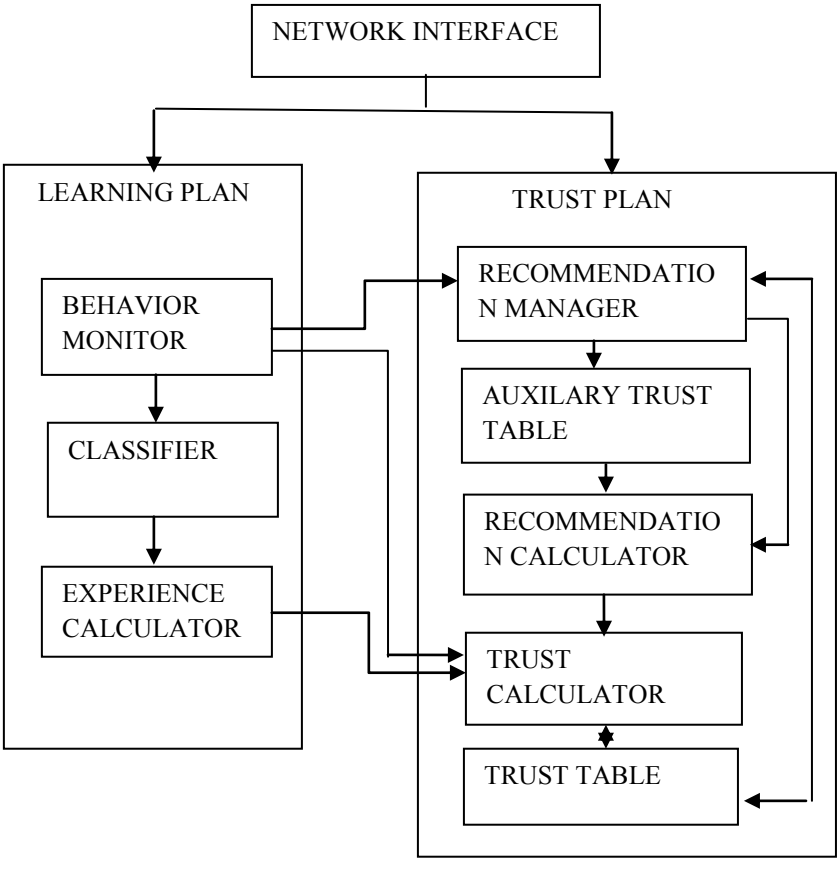


Fig. 4. Maturity Based Trust Model

(D) Working of REP in MANET

This protocol permits the nodes to interchange recommendations value between neighboring nodes. REP uses 3 messages, (i) Trust request (TREQ) (ii) Trust reply (TREP) (iii) Trust advertisement (TA)

Step 1 when new nodes (TN) come in network it sends TREQ message with IP address to each node

(- - - ➤)

Step 2 now neighboring node will only sends TREP with its recommendation value to

TN (target node) (⟶)

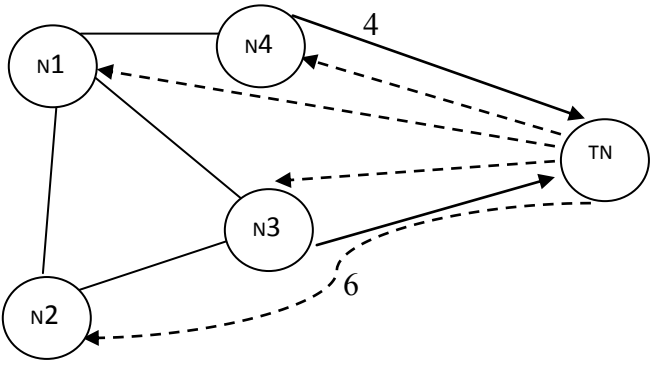


Fig. 5. Working of REP Protocol

Advantages: In this model no need of authentication mechanism. There is low vulnerability to false recommendation attack. It requires less resource consumption. This model is robust to slander colluding attack and tolerates up to 35% of liars. Any change in behavior of node can be easily identified by this model.

6 PKI Based Trust Model Scheme

The PKI approach in MANET can be implemented using either distributed certification or self organized public key management. In distributed certification scheme, by using a threshold digital signature, which provides facility of renewing & issuing, certificates [19-21]. Demerits: Needed additional storage requirement of public key. DOS attack not surely eliminated by this approach.

The self organized approach using centralized CA (certification authority) as self organized scenario [22]. Each node trusts on its neighboring node and stores information. The certificates receive trough chain of certificates which issued by nodes. According to [23], it uses this approach because of these reasons. All mobile nodes have equal roles. It requires less maintenance overhead. Simple bootstrap mechanism used in this scheme.

In This Approach, Each Node in MANET Performs These Tasks

Certificate Management: (i) Key generation, development of key pair (public key, private key) by node themselves (ii) Certificate issuance, public key with nodes identity binds in certificates, which issued by nodes it. (iii) Updated Certificate Repository, it is developed by node. (iv) Certificate exchange, non updated repository constructed by interchanging the certificates with other nodes.

Public Key verification: Searching and comparing the certificates in the chain. In algorithm, MPR technology used which was proposed by [23]. In MPR, the redundancy of messages can be decreased at local level. It search minimum number of nodes those required for reaching whole network, when applied recursively. For finding smallest number of certificates chain that is necessary to reach the node, algorithm: MPR Gout heuristic is used. This algorithm [23] defines re- transmission set for each vertex in certificate graph. Merits: Increment of certificate rate by using MPR technology. It reduced the length of certificate chain. Efficient verification procedure and authentication needs less communication between nodes.

7 Conclusion

In this paper, we surveyed existing trust schemes for mobile ad-hoc network to achieve the security and trustworthiness. It is concluded that, Protocol based trust scheme evaluate the trust through indirect communication but System level trust scheme is more feasible as compared to Protocol based. System level trust model uses concept of punishment or reward for nodes and it calculates trust value on the basis of direct communication. Cluster based and Maturity based model using standard eq. (1), (2) & (3) to find out trust value of node. Maturity based model is best as compared to Cluster based. In PKI based schemes, self organized scheme is more efficient than Distributed scheme of PKI. Some schemes like individual level trust model CRFSN, PTM etc, threshold cryptography, and cluster & non cluster based certification schemes in MANET are not covered in this paper. In future work, we plan to continue towards with unified trust model scheme.

References

1. Capra, L.: Toward a Human Trust Model for Mobile Ad-hoc Network. In: Proc. 2nd UK-UbiNet Workshop, May 5-7. Cambridge University, Cambridge (2004)
2. Jøsang, A., Presti, S.L.: Analyzing the Relationship between Risk and Trust. In: Jensen, C., Poslad, S., Dimitrakos, T. (eds.) iTrust 2004. LNCS, vol. 2995, pp. 135–145. Springer, Heidelberg (2004)
3. Golbeck, J.: Computing with Trust: Definition, Properties and Algorithm. In: Securecomm and Workshops- Security and Privacy for Emerging Areas in Communication Networks, Baltimore, MD, August 28-September 1, pp. 1–7 (2006)
4. 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)

5. Boukerche, A., Ren, Y.: A Security Management Scheme using a novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks. In: Proc. Int'l. Workshop on Modeling Analysis and Simulation of Wireless and Mobile System, Vancouver, British Columbia, Canada, pp. 88–95 (2008)
6. Yu, H., Shen, Z., Miao, C., Leung, C., Niyato, D.: A Survey of Trust and Reputation Management System in Wireless Communications. In: Proc. of the IEEE (2010)
7. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad-hoc Networks. In: ACM MobiCom Conference (2000)
8. Buchegger, S., Le Boudec, J.-Y.: Performance analysis of the confident protocol "(cooperation of nodes: fairness in dynamic ad-hoc networks)". In: IEEE/ACM Symposium on Mobile Ad-hoc Networking and Computing, MobiHoc 2002 (2002)
9. Michirardi, P., Molva, R.: Core: A collaborative reputation mechanism to encode node cooperation in mobile ad-hoc networks. In: CMS 2002 Communication and Multimedia Security Conference (2002)
10. Bansal, S., Baker, M.: Observation –based Cooperation Enforcement in Ad-hoc Networks, arxiv:cs/0307012v2 (2003)
11. He, Q., Wu, D., Khosla, P.: SORI: A Secure and Objective Reputation- based Incentive Schemes for Ad-hoc Networks. In: WCNC 2004 IEEE wireless Communications and Networking Conference (2004)
12. Hu, J., Burnmester, M.: LARS: a locally aware reputation system for mobile ad-hoc networks. In: 44th Annual ACM Southeast Regional Conference (2006)
13. Chen, A., Xu, G., Yang, Y.: A Cluster Based Trust Model For Mobile Ad-hoc Networks. IEEE (2008)
14. Cramp, R.: Logical foundations of probability. University of Chicago press (1950)
15. Cramp, R.: Replies and systematic expositions. In: Schilpp, P.A. (ed.) The Philosophy of Rudolf Carnap, pp. 966–998. Open court, La Salle (1963)
16. Velloso, P.B., Laufer, R.P., Cunha, D.d.O., Duarte, O.C.M.B., Pujolle, G.: Trust Management In Mobile Ad hoc Networks Using a Scalable Maturity Based Model. IEEE Transactions on Networks and Service Management 7(3), 172–185 (2010)
17. Virendra, M., Chanddrasekaran, M., Upadhyaya, S.: Quantifying trust in mobile ad-hoc networks. In: Proc. IEEE International Conf. Integration Knowledge Intensive Multi-Agent Syst., Waltham, USA (April 2005)
18. Theodorakopouls, G., Baras, J.S.: Trust Evaluation in ad-hoc networks. In: ACM Workshop Wireless Security (October 2004)
19. Saxena, N., Tsudik, G., Yi, J.H.: Threshold Cryptography in P2P and MANETs: the case of access control. Computer Networks 51(12), 3632–3649 (2007)
20. Wu, B., Wu, J., Fernadez, E.B., Ilyas, M., Magliveras, S.: Secure and efficient key management in Mobile ad hoc networks. Journal of Network Computer Applications 30(3), 937–954 (2007)
21. Joshi, D., Namuduri, K., Pendse, R.: Secure, redundant, and fully distributed ket management scheme in mobile and ad- hoc networks: an analysis. EURASIP Journal on Wireless Communications and Networking (4), 579–589 (2005)
22. Capkun, S., Buttyan, L., Hubaux, J.P.: Self-organized public key management for mobile ad-hoc networks. Mobile Computing and Communication Review 6(4) (2002)
23. Caballero-Gill, P., Herandez-Goya, C.: Efficient Public Key Certificate Management for Mobile Ad Hoc Networks. EURASIP Journal on Wireless Communications and Networking 2011, 1–10 (2010)