Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/4425
DOI URL: http://dx.doi.org/10.21474/IJAR01/4425
ISSN NO. 2320-5407

RESEARCH ARTICLE

SECURITY BREACHES IN TRUST MANAGEMENT SCHEMES IN MOBILE AD-HOC NETWORKS.

Bindiya Bhatia[1], Dr. M. K. Soni[2] and Dr. Parul Tomar[3].

1. Research Scholar, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Manav Rachna International University, Faridabad, 121001, India.
2. Professor & Dean, Department of Electronics Communication & Engineering, Faculty of Engineering & Technology, Manav Rachna International University, Faridabad, 121001, India.
3. Assistant Professor. Department of Computer Science & Engineering, YMCA University of Science & Technology, Faridabad, 121001, India.

Manuscript Info

Manuscript History

Received: 09 April 2017
Final Accepted: 11 May 2017
Published: June 2017

Key words:-
\Mobile Ad-hoc Networks, Trust Management, Uncertainty, Security attacks

Abstract

A Mobile Ad-Hoc Network allows distributed decision making by letting every node to take part in a routing decision. In this decision making the trust can play an important role. Establishing a trust among nodes is considered to be an influential tool to protect the wireless network. The nodes in the network can communicate with each other by building an acceptable level of trust relationships among themselves. But the trust management schemes themselves can be vulnerable to attacks. Trust Propagation and trust management in order to establish a trust, update a trust and revocation the trust is more challenging in a resource constrained MANET as compared to other traditional communication networks due to the dynamic topology change, mobility, conditions of propagation channels. In MANET, a malicious node can cause significant data damage and adversely influence the quality of the data. Thus, trust level analysis of a device can impact the certainty with which a device conducts data exchange with other device. The uncertainty and incompleteness of the trust evidence can be derived due to the dynamic characteristics of MANET. This paper is intended to pioneer the benefits of trust in MANET, investigate the various trust management schemes developed for MANET putting forward the summary of these techniques and the vulnerabilities associated with the trust management. The paper highlights the potential attacks and their impact on trust management in MANET.

Introduction:-

Mobile Ad-Hoc Network (MANET) is a resource constrained network. The devices are mobile and having limited bandwidth, computing power, memory. Besides this the network is having dynamic characteristics such as dynamic topology change, node failure, node mobility. Due to these characteristics, designing a security protocol is a challenging task in MANET for the security protocol Designers. Trust plays an important role to provide security to the network. Establishing a trust among nodes is considered to be an influential tool to protect the wireless network.

Corresponding Author:-Bindiya Bhatia.
Address:-Research Scholar, Department of Computer Science & Engineering, Faculty of Engineering & Technology, Manav Rachna International University, Faridabad, 121001, India.

The nodes in the network can communicate with each other by building an acceptable level of trust relationships among themselves. The notion of "Trust" initially gain attention from the social sciences and is delineated as the measure of belief about the behaviors of an independent entity. Blaze et al. [9] initially define the "Trust Management" and recognized it as a component of security in networks. There is a requirement of Trust propagation and management in MANETs is required whenever a node wants to interact with another node, and there is no previous interaction with that node. Initially the nodes formed a network with an adequate level of trust relationships among themselves. The trust management plays a significant role in many situations where decision has to take such as ensuring authentication, providing access control [28, 45], and effective routing [22,30]. The tasks involved in the Trust management are forming of trust level, propagating and updating the trust, and trust revocation. Managing & propagating the trust is more exigent task in MANET than in the networks having centralized environment. Node's mobility and dynamic change in the network affects the collection and propagation of trust information. In another case, due to the constraints of resources, the computation of the trust is based only on local information leads to the fact that establishing the trust can be relied on deficient and inaccurate information [11]. So the main aim of this paper is to study the vulnerabilities associated with the trust management in MANET. The paper is intended to define the trust in the wireless communication, to study the present techniques for trust management intended for MANETs, and to analyze the vulnerabilities that are associated with these techniques.

The paper is dividing in to 5 sections. In Section 2, trust is defined in context with wireless communication. Section 3 is presenting the various trust management schemes and the section 4 is analyzing the possible attacks that can breach the security. Section 5 is concluding the paper and presenting future directions.

Trust in Context of Wireless Communication:-

The trust can be defined in a different way in different fields. The section is presenting how a trust can be applied in a field of wireless communication.

Trust:-

There are multiple definitions of trust [13, 19, 49, 31]. In context of wireless networks Eschenauer et al. [11] defines the trust as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities." Trust can also be described as the degree of belief about the actions of other nodes.

All the data regarding the trust relationships is stored in a trust record. Relationship is set between two entities for a specific act. One entity builds a trust on another entity to perform an action. The first entity is considered as the subject and the second entity as the agent. Trust relationship can be represented by a notation: {subject: agent, action}. The level of trust is represented by the trust values associated with these trust relationship. The trust can be of two types: First, subject builds a direct trust after observing the behavior of the agent. Direct Trust is built if the interaction between the subject and the agents are successful. And second, when the subject has no direct relationship with the agent and the subject builds a trust on agent by getting the recommendations from other entities, called the indirect trust.

Direct trust is measured by beta distribution function [2] as:

$DT = s/(s+f)$

Where's' is number of successful interactions between subject and the agent and 'f' is number of failed interactions. Indirect Trust is building a trust using third parties. For example, if A has established trust on B and B trusts C, and then indirectly A builds a trust on C to a certain degree upon the recommendation of B. This phenomenon is called trust propagation. The propagation path can be single hop A-B-C or it can be multiple hops A-B-X-Y---C. It depend on the trust model how we calculate the indirect trust.

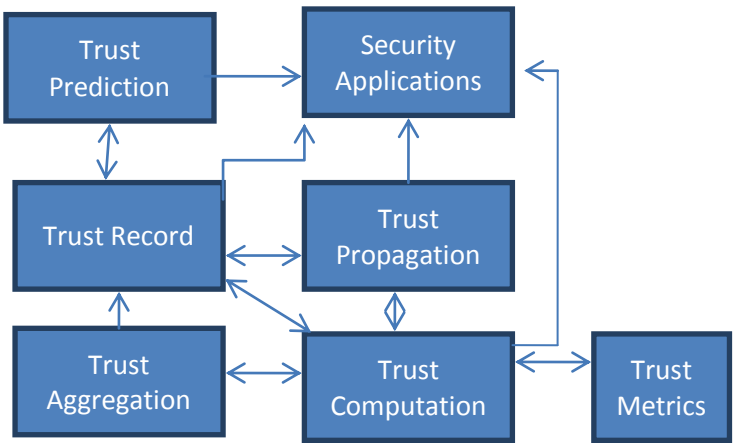

Figure 1:- Relationship between trust blocks.

Properties of Trust:-

Three major properties of trust are subject by Golbeck [15]: transitivity, asymmetry, and personalization.

Transitivity: First property says that the trust is not completely transitive in terms of mathematical logic. It says if A has established a trust on B and B has trust on A then it is not guaranteed that A has trust on C.

Asymmetry: Second property says that trust is not necessarily symmetric. It means trust is not identical to each other. This can be understood through the example of a trust relationship between a manager and an employee. A manager trusts an employee but it is not necessary that employee also trusts manager.

Personalization: Third property says that trust is inherently a personal opinion. The two entities can have different trust opinion on a particular entity.

Characteristics of Trust in MANETs:-

Trust can be characterized carefully in MANET due to its dynamic nature, unique and the inborn unreliability of the wireless medium. The main Characteristics of can be defines as [2, 10, 11, 23, 39]:

1. Trust evaluation method to build a trust against an entity should be fully distributed because there is no centralized entity in MANET.
2. Due to the resource constraints in MANET, the Trust should be evaluated without putting excessive computation and communication load.
3. The trust computation should not assume that the nodes will always be cooperative. The cooperation in MANET is not always necessary. In a resource constrained environment, nodes can acts selfishly in order to save the resources like battery and computation power.
4. Trust is not static, can change over time.
5. Trust is subjective.
6. Trust is context-dependent. A may trust B as a programmer but not as a designer. Like in MANETs, A having high computational power can be trusted by B because the task requires high computational power, while C having low computational power but not malicious can be distrusted.

Trust Management in MANET:-

This section is presenting the current techniques for trust management developed for MANET environments. Some of the trust management techniques have been proposed in order to present a general structure for distribution of trust evidence and trust evaluation in MANETs. Jiang and Baras [40] proposed an approach named ABED (Ant-Based trust Evidence Distribution) for trust distribution. The approach is based on highly distributed swarm intelligence model. The swarm intelligence concept is extensively used in the optimization problems that are dynamic in nature. (e.g. routing in wireless communication). The key principle behind the concept is stigmergy i.e. communicating indirectly through the environment. In ABED, the nodes can find the optimal path for gathering the trust evidence with the help of the information deposited by agents called ‘ants’’ But the scheme does not consider any specific attacks.

Theodorakopoulos and Baras [41] proposed a technique for assessment of trust evidence in MANETs. The assessment procedure is formed as a path problem in a directed graph where nodes and trust relationships among them are represented by entities and edges. The theory of Semirings is used to depict how the trust can be established between without previous direct interactions. GP web of trust is used to depict a trust model based on

Semirings and described that the projected method is robust in the existence of attackers. But the scheme assumes that trust is transitive. And the trust values are taken as binary instead of continuous-valued variable.

Recently Buckerche and Ren [42] proposed a scheme for distributed reputation evaluation named GRE (Generalized Reputation Evaluation) to efficiently avert the malevolent nodes from entering the trusted network. However, no specific attack model was addressed.

Marti et al[43] introduced an approach reputation-based trust management based on a watchdog that observes the node's actions and a route that gather reputation and get reply actions (e.g. finding malicious nodes as an outcome of misbehavior detection).

Michiardi et al [44] have given the proposal of a scheme named CORE (Collaborative Reputation) having a monitoring method with a reputation functionality that distinguish among direct reputation, indirect reputation, and functional reputation. The approach is built to formulate decision about consideration or separation of a node.
He et al. [45] introduced a trust management method based on trust management using an incentive mechanism, called SORI (Secure and Objective Reputation-based Incentive). This method support packet forwarding and discourage selfish behaviors based on quantified objective measures and reputation propagation by a one-way hash chain based authentication.

Nekkanti and Lee [46] extended AODV (Ad-hoc On-demand Distance Vector) by introducing trust aspect and security level at every node. In traditional AODV, routing information is encrypted which leads to huge overheads; the scheme use different stages of encryption based on the trust factor of a node, thus overhead is reduced.

Li et al. [47] also extended AODV and implemented a trust model to protect against malicious behaviors of nodes. In this scheme trust is represented as opinion. The opinion reflects the characteristics of trust in MANETs, particularly dynamicity.

Vulnerabilities Associated With Trust Management in MANET:-
Trust computation plays an important role in decision making, thus Trust evaluation, propagation and management playa are the major intention for the attackers. The section is analyzing vulnerabilities that are associated with attack then specifying the trust management schemes vulnerable to these attacks.

1. Denial of service attack (DOS): In order to consume the huge quantity of computing resources, the attacker sends large number of trust recommendation [53]. Thus as a result the target node enables to compute the trust value.
2. Bad mouthing attack (BMA): In Bad Mouthing attack, an intruder node give dishonest recommendations about the particular node and thus makes that node distrusted [54].
3. On-off attack (OOA): In this type of attacks, the malicious nodes act good and bad alternatively, in order to remain unnoticed while causing harms to the other nodes [55].
4. Conflicting behavior attack (CBA): In this attack, malevolent nodes act in a different way towards different nodes. The nodes can act inconsistently in different user domain causing confusion to the trust evaluation system. For example, a node can behave well with one group of nodes and badly with another group of nodes [56].
5. Sybil attack (SA): In this attack a malevolent entity forms many fake IDs. These IDs take the blame of being malicious, al malevolent node remains undetected [57], [58]. If the centralized entity is not there for authorization then it is easy to introduce Sybil attack in the network [59].
6. Camouflage attack (CA): In this attack, the malicious entity behave as per the majority entity and build trust. When they build enough trust, then they behave badly for specific tasks.
7. Collusion attack (CoA): In this attack, two or three malicious nodes can collaboratively give bad recommendation about the honest nodes and thus make the node distrusted.
8. Newcomer attacks (NCA): In the Newcomer attack, the intruder abscond the network and connect for a second time to wash out the prior corrupt record and to gain new trust [60].

The above mentioned vulnerabilities are associated with the trust management schemes. The table 1 is describing the trust management techniques and the vulnerable situation that these techniques not cater.

Table 1:- Analyzing the trust management models with its associated vulnerabilities.

Trust Management Model	Trust Properties	Attacks Considered	Vulnerabilities
Reputation based trust management using watchdog [48]	Dynamicity	Black hole	Bad Mouthing attack, Sybil attack, collusion attack
Extended DSR using hybrid scheme[49]	Transitivity, dynamicity	DoS	Bad Mouthing attack, Sybil attack, collusion attack
Extended DSR CONFIDANT Baysian Model incentive mechanism[50]	Transitivity, dynamicity	Route diversion	On-Off attack Sybil attack, Bad Mouthing attack
Context aware inference mechanism[51]	N/A	Packet Modification	Bad Mouthing Attack, conflicting behavior attack
Functional trust with a combination of direct observation and indirect information.[44]	Dynamicity, Personalization	DoS	Newcomer attack, Bad Mouthing Attack, conflicting behavior attack
Secure and Objective Reputation-based Incentive (SORI) [45]	Transitivity, asymmetry	False information propagation, Bad Mouthing Attack	Sybil Attack, Newcomer attack
Extended AODV based on trust aspect and security level[46]	Transitivity, asymmetry	DoS, Packet dropping	Bad Mouthing Attack, conflicting behavior attack
Extended AODV using subjective logic[47]	Transitivity, asymmetry, dynamicity	Detection of general malicious node	Bad Mouthing Attack, conflicting behavior attack, collusion attack, Sybil attack, on-off attack

The table is concluding that the trust management schemes in applicable in MANET are vulnerable to various security attacks. Although the schemes are securing the networks against some of the attacks but the application of these scheme also vulnerable to the various security breaches.

Conclusion:-

Trust management is a stimulating field of research. The eminent researcher's work moving around trust indicates its importance in MANET. Trust as a paradigm has an extensive variety of applications. The Main aim of this paper is to endow with MANETs designers with different perspectives of trust, its various properties and characteristics. The paper was started with the definition of trust in context with the wireless communication. Then, it presented the various existing trust evaluation and trust management schemes. And the analysis is done covering the vulnerabilities associated with trust management schemes. And during the analysis it was found that the trust management schemes are vulnerable to many attacks that can be considered in future to work upon. There are schemes that cater some of the attacks. But a complete solution is missing to provide a strong secure system.

References:-

1. Abdul-Rahman and S. Hailes, "Using Recommendations for Managing Trust in Distributed Systems," Proc. IEEE Malaysia Int'l Conf. on Communication (MICC'97), Kuala Lumpur, Malaysia, Aug. 1997.
2. W. J. Adams, N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," Proc. 6th Annual IEEE SMC Information Assurance Workshop (IAW'05), 15-17 June, 2005, West Point, NY, pp. 317-324.
3. E. Ahmed, K. Samad and W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks." AusCERT Asia Pacific Information Technology Security Conf., Gold Coast, Australia, 21-26 May 2006.

4. P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Mé, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches", Proc. 1st Int'l Workshop on Wireless Information Systems (WIS-2002), Apr. 2002, pp. 1-12.
5. Boukerche and Y. Ren, "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada, pp. 88-95, 2008.
6. S. Buchegger and J. –Y. Le Boudec, "Node Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," Proc. IEEE 10th Euromicro Workshop on Parallel, Distributed, and Network-based Processing, Canary Islands, Spain, Jan. 2002, pp. 403-410.
7. S. Buchegger and J. –Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks," Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing(MobiHOC), Lausanne, CH, 9-11 June 2002, pp. 226-236.
8. S. Buchegger and J.Y.L. Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems, 15 Nov. 2004.
9. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proc. IEEE Symposium on Security and Privacy, 6-8 May, 1996, pp. 164 – 173.
10. L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," Proc. 2nd UK-UbiNet Workshop, 5-7 May 2004, Cambridge University, Cambridge, UK.
11. L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.
12. Gahlin, "Secure Ad Hoc Networking," Master's Thesis, University of Umeå, March 2004. [13] Gambetta, "Can We Trust Trust?" Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 1990, pp. 213-237.
13. T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trust Routing Solution in Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 10, pp. 985-995, 2005.
14. J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks, Baltimore, MD, 28 Aug. – 1 Sep. 2006, pp. 1-7.
15. Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks," Proc. IEEE Wireless Communications and Networking Conf., vol. 2, pp. 825-830, March 2004.
16. K. Inkinen, "New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes," Seminar on Internetworking, Sjökulla, Finland, Spring 2004.
17. C. Kardof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 11 May 2003, pp. 113-117.
18. H. S. James, "The Trust Paradox: A Survey of Economic Inquiries into the Nature of Trust and Trustworthiness," Journal of Economic Behavior and Organization, vol. 47, no. 3, 2002.
19. T. Jiang and J. S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET," Proc. 2nd Int'l Conf. on Mobile Distributed Computing Systems Workshops (MDC), Tokyo, Japan, 23-24 March 2004, pp. 588-593.
20. Josang and S. LoPresti, "Analyzing the Relationship between Risk and Trust," Proc. 2nd Int'l Conf. Trust Management (iTrust'04), LNCS, Springer-Verlag, 2004, pp. 135-145.
21. J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks," IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.
22. R. Li, J. Li, P. Liu, H. H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," Proc. IEEE 65th Vehicular Technology Conf. (VTC'07), 22-25 Apr. 2007, pp. 56-60.
23. J. Liu and V. Issarny, "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks," Proc. 2nd Int'l Conf. of Trust Management (iTrust 2004), Oxford, UK, March 2004.
24. Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," Proc. 10th IEEE Int'l Workshop on Future Trends of Distributed Computing Systems, Sushou, China, 26-28 May 2004, pp. 80-85.
25. H. Li and M. Singhal, "Trust Management in Distributed Systems," Computers, vol. 40, no.2, Feb. 2007, pp. 45-53.
26. N. Luhmann, Trust and Power, Wiley, 1979.
27. H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Transactions on Networking (TON), vol. 12, no. 6, Dec. 2004, pp. 1049-1063.

28. S. Marsh, "Formalizing Trust as a Computational Concept," Department of Mathematics and Computer Science: University of Stirling, 1994.
29. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug. 2000, pp.255-265.
30. D. McKnight and N. Chevany, "The Meanings of Trust," Carlson School of Management, University of Minnesota, Technical Report TR 94-04, 1996.
31. R. Parasuraman, "Humans and Automation: Use, Misuse, Disuse, Abuse," Human Factors, vol. 39, no. 2, 1997, pp. 230-253.
32. K. Paul and D. Westhoff, "Context-Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks," Proc. IEEE Globecom Conf., Taipeh, Taiwan, 2002.
33. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad Hoc Networks," Proc. 27th Australasian Computer Science Conf. (ACSC), vol. 26, 2004, pp. 47-54. [35] A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-based Reactive Routing Protocols," IEEE Transactions on Mobile Computing, vol. 5, no. 6, June 2006, pp. 695-710.
34. T. Plesse, J. Lecomte, C. Adjih, M. Badel, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Plakoo, "OLSR Performance Measurement in a Military Mobile Ad Hoc Network," Proc. 24th Int'l Conf. on Distributed Computing Systems, 2004, pp. 704-709. [37] S. Ruohomaa and L. Kutvonen, "Trust Management Survey," P. Herrmann et al. (Eds.), iTrust 2005, Lecture Notes in Computer Science, vol. 3477, 2005, pp. 77-92.
35. Solhaug, D. Elgesem, and K. Stolen, "Why Trust is not proportional to Risk?" Proc. 2nd Int'l Conf. on Availability, Reliability, and Security (ARES'07), 10-13 April 2007, Vienna, Austria, pp. 11-18.
36. Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 305-317.
37. T. Jiang and J. S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET," Proc. 2nd Int'l Conf. on Mobile Distributed Computing Systems Workshops (MDC), Tokyo, Japan, 23-24 March 2004, pp. 588-593.
38. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, Feb. 2006, pp. 318- 328.
39. Boukerche and Y. Ren, "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, Vancouver, British Columbia, Canada, pp. 88-95, 2008.
40. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug.2000, pp. 255-265.
41. P. Michiardi and R.Molva,"CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-Hoc Networks," The 6th IFIP Conf. on Security Communications, and Multimedia, Porotoz, Slovenia, 2002.
42. Q. He, D.Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks," Proc. IEEE Wireless Communications and Networking Conf., vol.2, pp. 825-830, March2004.
43. R. K. Nekkanti andC. Lee,"Trust-based Adaptive On Demand Ad-Hoc Routing Protocol," Proc. 42th Annual ACM Southeast Regional Conf., Huntsville, Alabama, 2004, pp.88-93.
44. X. Li, M. R. Lyu and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad-Hoc Networks," Proc. 2004 IEEE Aerospace Conf., BugSky, Montana, 6-13 Mar. 2004, vol.2, pp.1286-1295.
45. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks, "Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug.2000, pp.255-265.
46. S. Buchegger and J.–Y. Le Boudec, "Node Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, "Proc. IEEE 10th Euromicro Workshop on Parallel, Distributed, and Network-based Processing, pp.403-410, Canary Islands, Spain, Jan.2002.
47. S. Buchegger and J.–Y. LeBoudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes-Fairness In Dynamic Ad-hoc Networks, "Proc. 3rd IEEE/ACM Symposium on Mobile AdHoc Networking and Computing, Lausanne, CH, 9-11 June 2002, pp.226-236.
48. K. Paul and D. Westhoff, "Context-Aware Detection of Selfish Nodes in DSR based Ad-Hoc Networks,"Proc. IEEE Globecom Conf., Taipeh, Taiwan, 2002.
49. P. Michiardi and R.Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperationin Mobile AdHoc Networks, "The 6th IFIP Conf. on Security Communications, and Multimedia, Porotoz, Slovenia, 2002.
50. J. Li, N. Li, X. Wang and T. Yu, "Denial of service attacks and defenses in decentralized trust management," in Secure comm and Workshops, 2006, pp. 1–12.

51. C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems," in The twenty first international conference on Information systems, ICIS '00, pp. 520–525, 2000.
52. L. F. Perrone and S. C. Nelson, "A study of on-off attack models for wireless ad-hoc networks," in First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks, 2006.
53. Y. L. Sun, Z. Han, W. Yu and K. J. Ray Liu, "Attacks on trust evaluation in distributed networks," in IEEE International Conference on Information Sciences and Systems, CISS, March 2006.
54. J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in The 3rd international symposium on Information processing in sensor networks, IPSN '04, pp. 259–268, 2004.
55. J. R. Douceur, "The sybil attack," in First International Workshop on Peer-to-Peer Systems, IPTPS '01, pp. 251–260, 2002.
56. J. D. Microsoft, J. R. Douceur, and J. S. Donath, "The sybil attack," in Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS), pp. 251–260, 2002.
57. P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems," Communications of the ACM, vol. 43, no. 12, pp. 45–48, 2000.