Intelligent Systems and Smart Infrastructure – Brijesh Mishra et al. (eds)

CHAPTER 45

Trust-Aware Mitigation of Various Security Threats for Internet of Things

Renu Mishra[1], Inderpreet Kaur[2]

Dept of CSE, Galgotia College of Eng. and Technology,
Gr Noida, India

Sandeep Saxena[3]

Dept of IT, IMS Unison University,
Dehradun, India

Raghwendra Mishra[4]

Dept of Mathematics,
Govt. PG College, Rudrapur, India

Tanu Shree[5]

Chandigagh University

Meena Sachdeva[6]

Dept of MCA, Galgotia College of Engineering and Technology,
Gr Noida, India

Abstract

Nowadays people want to enjoy the shift from "always on" to "always connected" communication environment. Internet fulfills that wish with full of capabilities to become an important part of next-generation wireless network. The similarity between any dynamic network and Internet of Things (IoTs) environment opens spick-and-span ways for providing different services in such environments and also focusses on various issues in its networking

Corresponding author: [1]renutrivedi11@gmail.com, [2]kaur.lamba@gmail.com, [3]sandeep.research29@gmail.com, [4]meetgirdhar@gmail.com, [5]tanu.shree29@gmail.com, [6]meena.sachdeva@galgotiacollege.edu

DOI: 10.1201/9781003357346-45

constraints as well. Ad hoc network is a dynamic and temporary network, which is settled on the fly without any skeleton. Usually they are used in military operations, emergency rescue, disaster recovery, wireless sensor network, and commercial multimedia communication. Due to open transmission medium and absence of secure boundaries, IoT became more susceptible to attacks with malicious intent to cripple the network. This chapter has the objective to highlight the benefits of soft security-based solution to provide the security in IoT environment during routing. The proposed trust-aware routing arranges all available routes in the descending order of trust value (TV) and ascending order of hop-counts.

Keywords: IoT, routing, trust, security, throughput

1. Introduction

Mobile Internet of Thing (IoT) is an ever-changing and non-permanent network, which is settled on the fly without any skeleton. Usually, they are used as a fast and short-lived communication network in hostile environments. The basic characteristics to provide flexibility and scalability are the uniqueness of this class of networks [1]. Similar to the traditional networks, security is a paramount concern in ad hoc networks also, with major security service requirements like confidentiality, authentication, authorization, and tamper proofing. Major challenges are faced while implementing any security solution for Mobile Ad Hoc Network in Internet of Things. Distributed operation is one of the main reasons to make the network open for criminals and attackers because no central controller is here; network controlling responsibilities of the network are distributed among all. The communication among nodes is cooperation based and each node can work as a relay, to implement routing and security. Multihop routing makes the network more vulnerable to various attacks caused by selfish and malicious nodes. A non-cooperative node in data transmission is called a selfish node, which saves the battery power for its operation. Data is forwarded either directly or via some intermediate nodes (if is not in its communication range). Since nodes can move arbitrarily, this makes the network topology very much uncertain. The medium is open to all nodes without any restriction. In most cases, IoT devices may be mobile, with limited CPU computation, low battery, and limited memory. Trust should be computed and evaluated between two neighbours in IoT's for security and reliable data transmission. It is also necessary to quantify the network behaviour in terms of "Trust", to improve security services. A comparison between Cryptographic and Trust-based Methods for MANET Routing Security is presented [2]. A set of parameters for the trust evaluation process can be defined to compute the overall trust to filtrate internal attacks and dishonest recommendations [28]. A node having less trust value (TV) is said to be malicious nodes that can drop the packet in between the network. Neighbour nodes are acrophobic to send the data even in the existing shortest path [30].

2. Literature Review

In any ad hoc type of networks, routing first does route discovery and then route maintenance. All prior routing methods presumptively presume that nodes are reliable and cooperative. This thought opens the door for vulnerability in the routing protocols. Because the nodes are not so powerful in terms of resources and infrastructure are barriers for high power-consuming cryptographic algorithms, so many crypto-based schemes are proposed to protect routing information but these approaches may not be suitable for real IoT. The power capacity of a mobile node affects network survivability in IoT since nodes will be disconnected if the battery is exhausted. An energy-efficient security should guarantee the long life of the network. An energy-efficient security protocol avoids downloading huge tables and limited calculations are preferred. We need a balanced approach that must be developed for secure computation and lifetime of the node [11]. Hard security protocols are not easy to implement and light security protocols can be easily attacked. Various mechanisms and protocols have already been advised for preserving energy and securing ad hoc networks. Researchers introduced trust-aware security for gaining confidentiality and authentication with Attack-tolerance, Compatibility, and Scalability. A comparison is presented [2] between Cryptographic and Trust-based security. Earlier, several issues like compromise node, computational overload, and energy preservation are highlighted. A lot of work was contributed to "lightweight" security mechanisms using trust [80]. They provide general ideas for trust evaluation in networks by applying different approaches. Some researchers proposed a trust model to establish trust in pure IoT [12]. The trust computation is based on monitoring data delivery in the network for secure routing evaluation in MANET. A new way to compute trust relationship to identifying malicious nodes in IoT was given in [13]. The trust-based mechanism includes the notion of friends, acquaintances, and strangers. These algorithms/protocols are not suitable for MANET with less power, storage, and processing. TSAODV [14] proposal came, in which information regarding routing having the highest trust value among all. One paper [15] utilized queuing theory as Trust Evaluation Factor; each node has k trust evaluation matrices which have many trust evaluation factors like paper link quality, distance, and mobility. Trust evaluation is being used in different new paradigms of networks like MANET, e-commerce, and other multiagent systems with different requirements. Different researchers contributed and presented various models to compute trust. Author M. Branchod gave CONFIDENT named contribution [16] to check the node's Fairness is the capital work for watchdog, trust/reputation manager. Trust ratings are computed and utilized in the routing process to increase the probability of detecting malicious nodes. In this area, researchers contributed a lot [17] [18] [19] but still we can't expect one all-round perfect solution that covers all fields. We can choose suitable features from multiple models to design the solution for our area. Various existing trust management schemes involved in major areas like routing and group communication and key management are investigated with their merits and demerits & findings. We identified some work [17, 20] in multi-criteria trust evaluation. Additionally, energy is included as an important QoS trust metric[21,22] to improve the performance of the network. In the literature review, we found that integration of different dimensions of trust is essential in the composition of a trust metric which would provide better performance. Taken all these facts into the account, we modified our early trust-based routing scheme [22]. Previously we proposed a trust-based model to

identify misbehaviour of the node by comparing the value threshold. However, this model was based single trust evaluation dimension to quantify and predict reliability among nodes. This single measure is not enough satisfactory in many scenarios (selfish behaviour, malicious intent, the lack of fixed infrastructure, limited resources, physical failures, etc.) of dynamic MANETs. Some modifications in the route discovery, trust update, and trust recommendation procedures are done to adjust the trust-aware communication. Lightweight trust-based routing protocol is proposed for mobile ad hoc networks, which consumes limited computational resource and suitable for blackhole and grey hole attack and specially to target denial-of-service attacks [23], [24]. Various attempts are made as an extension of AODV routing protocol with the help of direct trust and indirect trust. Direct trust is calculated from the number of packets received and forwarded, whereas Indirect trust is based on the reputation of the node, observed by other neighbour nodes. In ad hoc networks, securing routing protocols is one of the fundamental challenges.

It is simply an activity to shunt the legal policies on a system. An attacker may modify, release, insert false data, or obtain illegitimate access to disrupt network operation [2]. Since no central coordinating authority is present, the medium shared in the IoT makes it more vulnerable than wired networks. The apprehension of possible attacks will ever be the first step in the direction of designing a good security policy. External and internal attacks are the two types of attacks. An outsider can cause congestion or spread misleading routing information in an external assault. On the other hand, the internal attacks are committed by compromised member nodes, which may gain access and pretend to be authorized node [3].

A. Popular Attacks in IoT

Here are some popular attacks on the routing protocols:

1. *Black Hole Attack:* In this, the attacker node publicizes itself for having the shortest route to any desired node in the network. Normal innocent nodes rely on the received reply as they follow cooperation-based forwarding. Malicious node takes advantage of this and replies to the request, claiming for having the shortest path [4]. Source node has to trust that reply in the absence of verifying mechanism. The network can be targeted by a single black hole node or a group of attacker nodes that work together to degrade the network reliability.
2. *Gray Hole Attack:* It is a special case of blackhole attack by dropping a few packets with a set of probability [5]. The node may drop some or all the packets for some time and later behave very normal.
3. *Rushing Attack:* A malicious node rising the speed (Rush) of the routing process. It accepts the Route Request packet and forwards to its neighbours sooner as compared to others. The packet from the attacker will reach first and will be accepted and other RR will be discarded with source sequence numbers.
4. *Wormhole Attack:* Wormhole attack catches the packet from one location and sends it over the tunnel to the other location. The tunnel is planned to give the impression of having the optimized path to the destination. It happens with the help of multiple

malicious nodes, which may create choke points [6]. A wormhole attack may equally harm to proactive and reactive protocols both.

5. *Sybil Attack:* Here attacker node controls multiple identities by assuming arbitrary identities or may spoof legitimate nodes. This attack can be launched either to erase the proofs of its earlier malicious activities or to disrupt the network.

3. Security Countermeasures in IoT

Designing the adequate security framework is very hard in IoT because no such strong boundary exist to separate insider nodes from outside network. An idiosyncratic security solution is not enough due to no stability of nodes and is incapable of physical protection to catch security threats [29]. Additionally, because the ad hoc network is distributed and infrastructure-less networks, it might be best to implement security strategies at the individual node level in below two dimensions [22].

A. Cryptography (Hard Security)

Cryptography is just an art of hiding information. It works as an important security tool to provide authentication, confidentiality and other services [7]. There are two popular approaches to implement cryptography. First is a symmetric type where the same key supports encryption and decryption, while the public/asymmetric approach is based on different keys to encrypt and decrypt the data [8], [26], [27]. Although asymmetric cryptography is versatile (authentication, integrity, and confidentiality) and simple to use for key distribution, it is not without flaws. Single key cryptographic algorithms have lighter computation than the public-key approach but suffer from a key compromise problem. Any cryptosystem trusts on some inherent efficient key management system.

B. Trust Evaluation (Soft Security)

Various cryptographic algorithms are proposed to provide secure solutions but often seem unfeasible because they assume that nodes are cooperative and trustworthy [9]. The importance of trust management is realized and followed by society to design better security protocols. It is an approved tool to mitigate attacks and filter out misbehaving nodes based on social properties, each node is going to be assessed with the threshold value [10], and the isolation of node is performed by trust value. Any trust-based security solution aims to provide a performance guarantee through the evaluation of node behavior. Current routing algorithms aim only to find optimal routes but not cover performance guarantee. Widespread use of IoT creates the need for a system to rank out the behavior of the network. Here, multidimensional trust evaluation scheme is designed by including current attributes (Direct Trust) of node and the past behavior (Indirect Trust) with others to improve Quality of Service (QoS) [25].

4. Proposed Routing for Trust-based Security

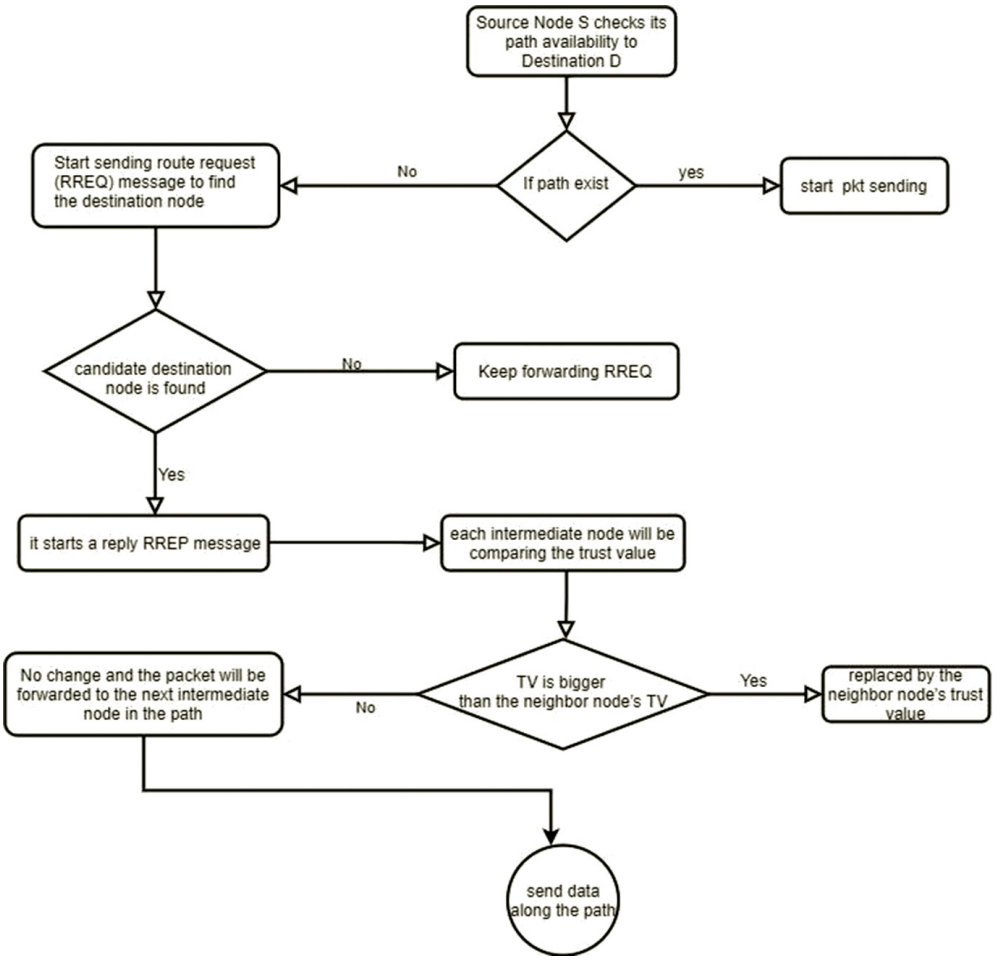

Fig. 45.1 Flow Chart for Trust-based Proposed Routing

Stage 1: Source node A will send RREQ packet to B and C, which are neighbors of it and it will continue till reaching the destination. After reaching the destination, the destination sends Rtrep packet back to source A. Rtrep packets are broadcasted from various paths over a specified time.

Go get trust-aware route; all available routes are arranged as per the descending order of TV and ascending order of hop-counts. Whenever a fresh route is found, in this stage, it could be ensured that the chosen routes are with minimum hop-count and highest TV.

Stage 2: Now, the first route is chosen and the first part of the message is routed. Similarly, the next route is chosen with a similar assumption. If all the message parts securely routed, the real routing is accomplished by chosen paths.

Stage 3: If more paths are chosen over possible eligible paths, set all these paths in their energy that need to transmit the packets. Then, choose the lowest energy path and so on.

Stage 4: Repeat until secure routes are obtained.

Stage 5: The algorithm is repeated from Stage 2 by choosing an alternate route if no secure routes are available.

Stage 6: This mechanism works until all the paths are drained. Moreover, the mechanism halts for another route if no secure route is obtained. Also, it can be assumed that the algorithm could fail if all routes are available, or a specific time interval is no longer valid.

5. Experimental Setup

On the basis of the following metrics, we compared our proposal to the normal DSR and normal AODV using the ns 2.34 simulator. The maximum node speed is set to 10 m/s, and the percentage of malicious nodes in the network is set at 10% of all nodes. We experiment with different network sizes to see how they affect the results.

As shown in Fig. 45.2, a total of 19 IoT nodes are participating in such environment and device 10 wants to send any routing packet to receiver device 19. Each node has its trust value; on the basis of the predefined threshold, only few nodes have qualified. Next step is to update the routing information with only qualified nodes.

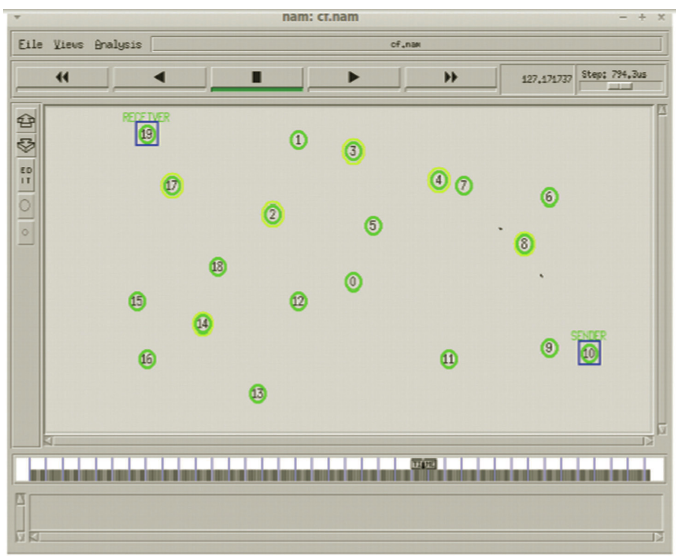

Fig. 45.2 Environmental Setup

Throughput: We evaluated the throughput of the proposed scheme with the conventional AODV routing.

Throughput = Total packets received/Total packets sent

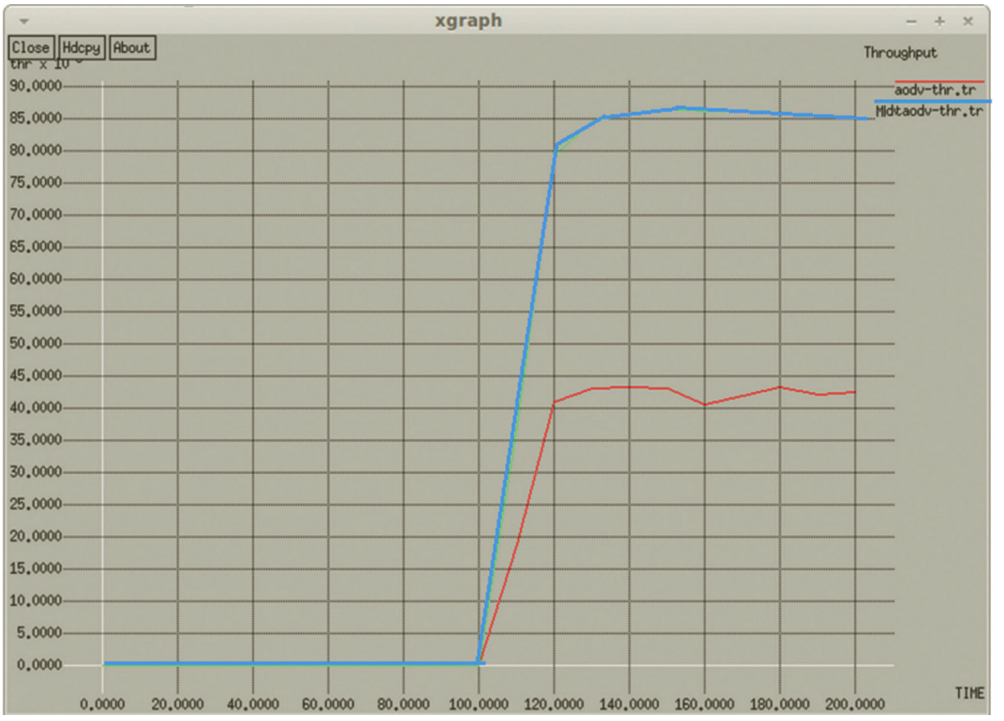

Fig. 45.3 Throughput Comparison

Delay: Delay means the time period to route a packet. Our second evaluation is done on the delay in both the routing algorithms.

Delay = Number of sending bits in the packet/Throughput

6. Conclusions

The paper tries to explore the importance of trust-based security solution with the token of proof. The Throughput and Delay are the two factors to prove that the proposed trust-based AODV gave better performance in such IoT. Environment is depicted in diagrams 5.2 and 5.3, respectively, in the above result analysis section. Trust concepts are proved as a better way to achieve security in various operations related to network communication like routing, data collection, and more. Man-in-the-middle, black hole, and Denial of service attacks are accrued very frequently just because of the pre-assumption about cooperation and trustworthiness of nodes. The paper firstly discusses IoT and how Trust works in case of such ad hoc networks.

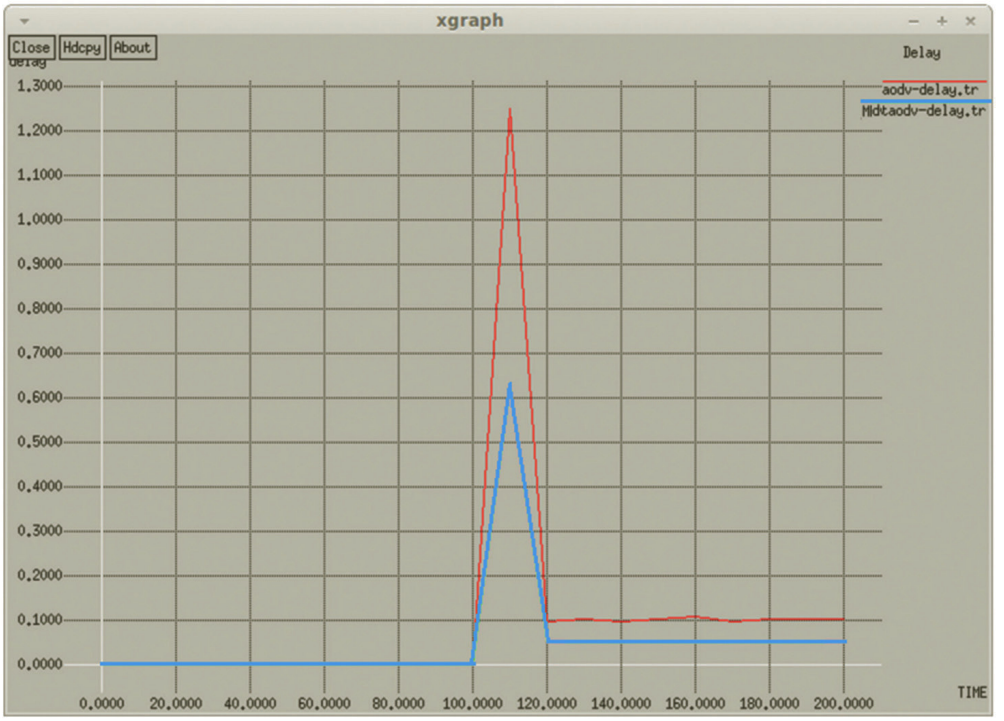

Fig. 45.4 Delay Comparison

In various sections, we identified the most possible attacks for MANETs and discuss their countermeasures. Trust-based security solutions are reviewed and declared as one of the best security solutions for such dynamic and modern environment. It investigates in detail the management of Trust through related works. Trust-based schemes are attack-tolerant, cooperative, flexible, lightweight, and scalable as well as compatible to the rapidly growing network size.

7. Acknowledgment

First of all, we would thank the Almighty GOD who has always blessed me by granting his kindness to complete the task. I would like to state my gratitude to Dr. Niraj Kumar Shukla for providing such platform.

References

1. A. Gupta, P. Verma, and G. Sambyal, "An Overview of MANET: Features, Challenges and Applications," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 4, no. 1, pp. 122–126, 2018J.

2. Cordasco and S. Wetzel, "Cryptographic versus trustbased methods for MANET routing security," ElectronicNotes in Theoretical Computer Science, vol. 197, no. 2, pp. 131-140,2008.
3. R. J.Lewicki and B.B. Bunker, "Trust in Relationships: A Model of Trust Development and Decline, In Conflict, Cooperation and Justice, B. Z. Rubin, Ed. San Francisco: Jossey-Bass, 1995,pp.133-173.
4. C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," Computer Networks, vol. 113,pp.94-110,2017.
5. N. A. Funde and P. Pardhi, "Detection & prevention techniques to black & gray hole attacks in MANET: a survey," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 10, pp.4132-36,2013.
6. N. Gupta and S. N. Singh, "Wormhole attacks in MANET," in 2016 6th International Conference-Cloud System andBig DataEngineering (Confluence),2016:IEEE, pp.236-239.
7. J. Lindley-French, "The Revolution in security affairs: hard and soft security dynamics in the 21st century," Europeansecurity,vol.13,no.1-2,pp.1-15,2004.
8. A. Kahate, Cryptography and network security. Tata McGraw-Hill Education,2013.
9. K. Garg and M. Misra, "Trust based security in MANET routing protocols: a survey," in Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India,2010,pp.1-7.
10. M. Branchaud and S. Flinn, "xTrust: A Scalable Trust Management Infrastructure," in PST, 2004, vol. 4, pp. 207-218.
11. M. A. Morid and M. Shajari, "An enhanced ecommerce trust model for community based centralized systems," Electronic Commerce Research, vol. 12,no. 4, pp. 409-427,2012.
12. A. Sharma and D. N. Kumar, "Trust Based Theoretical Framework for Mobile Ad-Hoc Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, pp. 905909,2013.
13. S. Sridhar, R. Baskaran, and P. Chandrasekar, "Energy supported AODV (EN-AODV) for QoS routing in MANET," Procedia-Social and Behavioral Sciences, vol. 73,pp.294-301,2013.
14. D. K. Prasadh and R. Senthilkumar, "Nonhomogeneous Network Traffic Control System Using Queueing Theory," International Journal of Computer Engineering & Technology (IJCET), vol. 3, no. 3, pp. 394405,2012. are using a style other than Chicago Manual of Style, 16th edition so we can ensure it is retained).
15. A. Verma and M. S. Gujral, "Trust Oriented Security Framework for Ad Hoc Network," Journal of Computer Science & Information Technology, vol. 5, pp. 19-26,2012.
16. M. Branchaud and S. Flinn, "xTrust: A Scalable Trust Management Infrastructure," in PST, 2004, vol. 4, pp. 207-218.
17. K.S.Ramana,A.Chari,andN.Kasiviswanth,"Asurveyontrustmanagementformobileadhocnetworks," International Journal of Network Security & Its Applications(IJNSA),vol.2,no.2,pp.75-85,2010.
18. K. S. Ramana, A. Chari, and N. Kasiviswanth, "Trust based security routing in mobile adhoc networks," IJCSE) International Journal on Computer Science and Engineering,vol. 2,no.02,pp.259-263,2010.
19. N. K. Nehra, M. Kumar, and R. Patel, "Neural network based energy efficient clustering and routing in wireless sensor networks," in 2009 First International Conference on Networks & Communications, 2009: IEEE, pp.34-39.
20. A. Ahmed, P. Kumar, A. R. Bhangwar, and M. I. Channa, "A secure and QoS aware routing protocol for Wireless Sensor Network," in 2016 11th International Conference for Internet Technology and Secured Transactions(ICITST),2016:IEEE,pp.313-317.
21. N. C. Fernandes and O. C. M. B. Duarte, "An efficient group key management for secure routing in ad hoc networks," in IEEE GLOBECOM 2008-2008 IEEE Global elecommunicationsConference,2008:IEEE,pp.1–5.

22. R. Mishra, I. Kaur, and S. Sharma, "New trust based security method for mobile ad-hoc networks," International Journal of Computer Science and Security (IJCS), vol. 4, no. 3, p. 346, 2010.
23. I. Kaur, "A Survey to Improve the Network Security with Less Mobility and Key Management in MANET,"2018.
24. S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in MANET," in 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017: IEEE, pp. 818–824.
25. M. Maleki, K. Dantu, and M. Pedram, "Power aware source routing protocol for mobile ad hoc networks," in Proceedings of the 2002 international symposium on Low power electronics and design, 2002, pp. 72–75.
26. S. Taneja and A. Kush, "Energy efficient, secure and stable routing protocol for MANET," Global journal of computer science and technology, 2012.
27. T. Singh, J. Singh, and S. Sharma, "Energy efficient secured routing protocol for MANETs," Wireless Networks, vol. 23, no. 4, pp. 1001–1009, 2017.
28. S. Hammer, M. Wißner, and E. André, "Trust based decision-making for smart and adaptive environments," User Modeling and User-Adapted Interaction, vol. 25, no. 3, pp. 267–293, 2015.
29. M. Cukier and S. Panjwani, "A Comparison between Internal and External Malicious Traffic," in The 18th IEEE International Symposium on Software Reliability (ISSRE'07), 2007: IEEE, pp. 109–114.
30. A. Lamba, S. Garg, and R. Kumar, "A Literature Review of MANET's Routing Protocols Along With Security Issues," 2016.
31. D. Geetha and S. Sakthivel, "Service Orient Stream Cipher Based Key Management Scheme for Secure Data Access Control Using Elliptic Curve Cryptography in Wireless Broadcast Networks," American-Eurasian Journal of Scientific Research, vol. 11, no. 1, pp. 63–71, 2016.
32. H. Kojima, N. Yanai, and J. P. Cruz, "ISDSR+: Improving the Security and Availability of Secure Routing Protocol,"IEEE Access,vol. 7, pp. 74849–74868, 2019.
33. K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in 2008 4th international conference on wireless communications, networking and mobile computing, 2008: IEEE, pp. 1–5.
34. K. K. Chauhan and A. K. S. Sanger, "Securing mobile Ad hoc networks: key management and routing," arXivpreprintarXiv:1205.2432,2012.
35. N. Bißmeyer,S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in vanets using data plausibility checks with particle filters," in 2012 IEEE Vehicular Networking Conference (VNC), 2012: IEEE, pp. 78–85.
36. R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Integrated social and quality of service trust management of mobile groups in ad hoc networks," in 2013 9th International Conference on Information, Communications &Signal Processing, 2013: IEEE, pp. 1–5.
37. R. Menaka, V. Ranganathan, and B. Sowmya, "Improving performance through reputation based routing protocol for manet," Wireless Personal Communications, vol. 94, no. 4, pp. 2275–2290, 2017.
38. Rao, PV Venkateswara, and S. Pallam Setty. "Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non Responsive Traffic." International Journal of Computer Applications 120.22(2015)
39. S. Ba and P. A. Pavlou, "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior, MIS Quarterly, Vol. 26, pp. 243–268, 2002.
40. D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial Trust Formation in New Organization Relationships, Academy of Management Review, Vol. 23, pp. 473–490, 1998 Common reference uses for the Chicago Manual of Style, 16th Edition are below. If you require information on a different style, please contact your Project Coordinator.