A Survey on Trust Evaluation in Mobile Ad Hoc Networks

Guangwu Xu
State Key Laboratory on Integrated Services Networks
Xidian University
Xi'an, China
xuguangwu_china@163.com

Zheng Yan
State Key Laboratory on Integrated Services Networks
Xidian University, Xi'an, China
Department of Communications and Networking
Aalto University, Espoo, Finland
zyan@xidian.edu.cn

ABSTRACT
Mobile Ad Hoc Network (MANET) is a multi-hop temporary and autonomic network comprised of a set of mobile nodes. MANETs have the features of non-center, dynamically changing topology, multi-hop routing, mobile nodes, limited resources and so on, which make it face more threats. Trust evaluation is used to support nodes to cooperate in a secure and trustworthy way through evaluating the trust of participating nodes in MANETs. However, many trust evaluation models proposed for MANETs still have many problems and shortcomings. In this paper, we review the existing researches, then analyze and compare the proposed trust evaluation models by presenting and applying uniform criteria in order to point out a number of open issues and challenges and suggest future research trends.

CCS Concepts
General and reference~Surveys and overviews • General and reference~Evaluation

Keywords
Trust Management, MANET, Trust Evaluation, Privacy Preservation

1. INTRODUCTION
Mobile ad hoc network is a multi-hop, self-organizing system that is made up of a group of mobile terminals with a routing function, in which mobile nodes communicate with each other without center and fixed infrastructure. It has characteristics such as multiple hops, reciprocity, rapid deployment, self-organization and low construction costs, compared to traditional networks. MANETs enable mobile users to share and distribute contents through direct mobile-to-mobile wireless connections. With the miniaturization and popularity of mobile devices in recent years, MANETs have begun to participate in the establishment of personal communication networks and become an important form of network access for mobile communications.

In spite of the significant benefits of MANETs, MANETs are faced with many serious security problems, due to its special characteristics. As described in [1,5,12], MANETs are vulnerable to many attacks raised by malicious nodes, such as rushing, packet dropping, packet flooding, DoS/DDoS, blackholes, due to multi-hop routing and absence of any trusted third party in such an open environment. In response to these security issues, a lot of researches were conducted, mainly from the aspects of trust model, routing protocol, key management, intrusion detection and authentication of MANETs. The security solutions proposed for other kinds of systems or traditional networks are mostly not suitable to be applied into MANETs. Trust evaluation is an important and effective solution for nodes to identify and avoid malicious nodes and ensure effective interactions among the participating agents in MANETs. Trust evaluation(TE) in MANETs aims to collect trust evidences and evaluate or measure the trust levels of mobile nodes, which plays an important role in MANETs for trusted route selection, qualified services with context-aware intelligence, and to assist secure interactions between mobile nodes. The trust information and evidence used for trust evaluation are only provided by the nodes in the network [5, 17]. Trust models can help terminals to decide whom to trust, encourage trustworthy behavior, and discourage participation by nodes that are dishonest. However, trust is a complicated concept with regard to the confidence, belief, and expectation on the reliability, integrity, dependability, ability, and other characters of an entity. And the relationship between a trustor and a trustee in MANETs has the basic features such as subjective, dynamic, and context-aware. Due to these features, there are problems that traditional way of resisting attack cannot holistically consider the impact factors of trust and have some other deficiencies. As a result, they cannot properly prevent selfish, malicious and compromised nodes wrapped in a number of authorized participants in the network from behaving maliciously. Even though many trust evaluation models and trust management schemes in MANETs have been proposed now, the performance of these models is undesirable. This fact severely hinders the development and successful deployment of MANETs. Therefore, it is still essential for us to review existing trust evaluation models based on uniform criteria in order to figure out open issues and direct future research focuses.

In this paper, we conduct an extensive survey on trust evaluation models and mechanisms in MANETs. We propose uniform criteria to evaluate the performance of trust evaluation models, which concerns almost all aspects that may influence trust. Then based on a literature review and analysis, we point out a number of open issues and challenges and suggest future research trends related to trust evaluation in MANETS.

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China
Copyright © 2016 EAI
DOI 10.4108/eai.18-6-2016.2264132

The rest of the paper is organized as follows. Section 2 introduces the basic concepts of trust evaluation and proposes uniform criteria for assessment on trust evaluation in MANETs. An overview of the literature about trust evaluation in MANETs is presented in Section 3 with comparisons and analysis. Section 4 specifies a number of open research issues and discusses research challenges and future research trends. Conclusion is given in the last section.

2. BASIC CONCEPTS AND TRUST EVALUATION CRITERIA IN MANETs

2.1 Basic Concepts

Trust*:* Trust has been defined in many disciplines, such as sociology, psychology, computer science, etc. In psychology, trust is considered to be a psychological state of the individual, where the trustor risks being vulnerable to the trustee based on positive expectations of the trustee's intentions or behavior. In sociology, trust is defined as "a bet about the future contingent actions of the trustee". Herein, we take the natural definition of ''trust''. Trust is a substantive evaluation of subjective probability of another entity will perform a behavior of a specific. This assessment is observed before actual behaviors, which is context-dependent [16]. Trust can be classified into two types according to different information sources: one is direct trust; the other is indirect trust [3, 11]. Direct trust is a kind of independent trust of the node's credibility on the other nodes, which is based on direct interaction experiences with other nodes, observing each other good and bad behaviors so as to establish the degree of trust in other nodes. Indirect trust is some node trust other nodes in some degree, trust the source of information is information from other nodes, the information can be in the form of their own direct trust and can also be the information they collected from other nodes.

From the above definition, we can see that trust is subjective on one hand. Different entities could hold different trust in the same target entity. Trust is a subjective phenomenon based on many factors or evidence. On the other hand trust is context-dependent. Any trust is associated with a certain context, such as the one that is credible to an entity or not.

Trust Evaluation: There are many different methods to compute the degree of trust in distributed networks, like MANETs. We adopt the idea that trust is composed of two parts: direct trust and indirect trust, like reputation and recommendation. Trust evaluation is an essential part of trust management to aid decision-making.

In a centralized model of trust evaluation, trust values are maintained in a common central node or through an authorized third party. The simplest method is to sum the number of positive ratings and negative ones separately and keep a total score that equals to the positive score minus the negative score. However, MANETs have the feature of non-center, this goes against the requirement of a trusted third party.

In a decentralized model of trust evaluation, a node assigns a trust value for every communicated node. Some researchers advocated the use of ratings and prefer to complex rating aggregation algorithms to evaluate from several aspects and filter out the bad ratings [6]. However, these sophisticated models are not appropriate for MANETs where resources are scarce and network topology is dynamic. Although in principle these models could be applied in routing in MANETs, additional recommendation information exchanging incurs significant network overhead.

Trust Management*:* Trust management concerns using a unified approach to describe, explain and manage trust policies, trust credentials and trust relationships for the direct authorization of critical security operations [9, 15, 16].

Trust Model*:* The trust model essentially performs the function of trust derivation, computation, and application. In MANETs, each node could derive trust factors from packet forwarding ratio and others, to estimate the overall trust in a node based on trust evaluation, and compute a routing path's trust. Currently trust model plays an important role in securing a networking system, especially those with no centralized third trusted party to rely on.

The measurement and computation of trust to secure interactions between mobile nodes are crucial for the development of MANETs. Many trust models have been proposed in existing researches. However, these models are not always suitable for MANETs. Most of the proposed models just analyze trust issue from some points of view in MANETs. It still lacks a comprehensive study to show if the existing solutions are sufficient enough for achieving trustworthy MANETs. Therefore, it is essential to review the state of trust evaluation in MANETs in order to figure out open issues in this research field and motivate future research and investigation.

2.2 Criteria of Trust Evaluation in MANETs

Herein, we propose a number of criteria for assessing the performance of trust evaluation models in MANETs. The purpose is to use a uniform research model to figure out potential problems of current research in order to find open research issues and direct future research.

Trustworthiness (T): The trust evaluation should be robust to overcome various potential attacks on it, such bad-mouthing attacks, conflict behavior attacks, on-off attacks, etc.

Adaptability (Ad): In MANETs, the trust relationships among nodes could be dynamically changed due to node joining and leaving. Since trust is context-aware, it is essential for trust evaluation to be adaptive to context changes.

Usability (Us): MANETs are normally applied to provide intelligent services by interacting with human beings. Users should drive the design of trust solutions if they are related to the MANET node users. This concern is caused by the subjective characteristic of trust.

Privacy (P): User privacy should be preserved when node user data are collected for trust evaluation. Trust evaluation in MANETs should allow the legitimate users to preserve their privacy to a maximum extent.

Accuracy (Ac): The accuracy of trust/reputation evaluation should be ensured without any doubt.

Efficiency (E): Trust evaluation should be efficient in order to dynamically manage trust relationships in MANETs for the purpose of ensuring networking security.

Uniformity (Un): It is preferred to offer a uniform model to consider node users subjective voting with trusted credibility for trust evaluation.

Comprehension (C): The trust evaluation should concern various trust influencing factors in a comprehensive way. This is essential for achieving accurate trust evaluation.

Generality (G): Trust evaluation for various MANET systems and services can be commonly or widely used in different application scenarios, which is a preferred objective for trust evaluation.

3. LITERATURE REVIEW

In this section, we review the recent literature about trust evaluation in MANETs. Our review is based on the study on the papers published in recent 10 years searched and selected from the following database: IEEE Explorer, ACM library, Springer library, Engineering Village and Web of Science by using the following keywords: trust, trust evaluation, trust management, trust model, reputation generation, reputation assessment, reputation evaluation, reputation system and MANET.

We summarize trust evaluation models that have been developed for MANETs in this section by classifying them into reputation-based trust models and policy-based trust models according to the generation of final trust value. Further, we also describe and analyze existing trust models for trust (or reputation) evaluation based on the proposed criteria.

3.1 Reputation-Based Trust Models

Most reputation-based trust models calculate reputation and trust by collecting, aggregating and distributing user feedback and disseminating reputation among MANET nodes. A reputation based trust model for MANETs can cooperatively help to exclude distrusted nodes from the network while tolerating transient faults sometimes. These models help nodes decide whether one node is trusted, thus they can encourage trustworthy behaviors and discourage the participation of dishonest nodes. Reputation-based trust models utilize numerical and computational mechanisms to evaluate trust.

3.1.1 Objective Reputation-Based Trust Models

In [1], a reputation-based trust management system was proposed for detecting and preventing MANET vulnerabilities; it can detect attacks in a purely distributed manner through collaborative monitoring information exchange among nodes. The performance of the simulation showed an improvement to detect misbehaving nodes and malicious nodes considering various trust factors in a dynamic environment, compared with trust models that not use this scheme. Therefore, this system satisfies the criterion of trustworthiness partially and comprehension. It tested the performance in various attack scenarios, so it satisfies adaptability. And, trust model with this scheme show a good performance in delivery ratio, lower packet-loss rate detection rate, throughput. Therefore, it satisfies the criterion of accuracy and efficiency. And it didn't support subjective opinion or voting and privacy preserving, so it do not conform the criterion of uniformity and privacy. Although the scheme shows the advantages of packet delivery rate and can investigate the attacks raised by malicious, selfish and misbehaving nodes, it did not consider and test in different MANET application scenarios, the criterion generality was not considered. Moreover, the scheme is fixed, users cannot drive the design of trust solutions, and therefore the usability has not yet been considered.

Kpodjedo, Pierre and Pourzandi proposed a trust evaluation scheme called RTA in MANETs based on the reputation of node's software composition [8]. The trust evidence collection result, reputation values for different software components of mobile terminals are stored in the reputation database module, based on a reliable and credible reporting scheme for integrity measurement. The simulation of RTA in [8] demonstrated great efficiency at detecting malicious software of highly mobile MANET nodes. Therefore, it satisfies accuracy and efficiency. And as it only focus on malicious software, other attacks are not considered, trustworthiness is partially satisfied. Because of the topology in the simulation is changeable and the scheme can perform well, which proofs it can aware the dynamic situation, so it satisfies the criterion of adaptability. The proposed trust evaluation scheme is fixed and user cannot configure the trust solution, it doesn't satisfy usability. This work didn't take into consideration the issue of privacy preserving. The scheme doesn't support subjective view and voting, so it cannot conform uniformity. The test scenario was fixed, without consideration on generality. In the simulation, the considered trust factor is only integrity measurement, subjective view and recommend value were not considered, so it does not satisfy the criterion of comprehension.

Boukerche and Ren proposed a distributed reputation evaluation mechanism called Generalized Reputation Evaluation (GRE), which is a trust-based integrated computing reputation model [3]. In this system, terminals' historical reputation records were considered in trust calculation, which indeed have a significant effect on its current trust. It makes aware historical trust of participating nodes, therefore this trust model satisfies adaptability. Reputation assistant mechanism in [3] can significantly reduce the impact of malicious evaluation from malicious nodes and obtain a more realistic value of trust, which shows it satisfied accuracy. This scheme achieved that the nodes who have a low initial or previous trust values would not have high past trust records, in this case, the trust model would not increase their reputations in a high speed. Simulation result indicated that this reputation evaluation model could calculate efficiently the trustworthiness of wireless and mobile devices. Therefore it satisfies trustworthiness and efficiency. It didn't consider privacy preserving, so the criterion privacy is not satisfied at least not very well. Since users cannot personalize this trust model, the usability criterion is not satisfied. One problem is that the scheme does not include a mechanism support subjective view or voting, thus, it does not satisfy uniformity. It did not consider and test in many MANET application scenarios, generality was not considered.

3.1.2 Subjective Consciousness-Based Trust Models

In most reputation-based frameworks, confidence values and willingness of users, which are important parameters, were not considered, such as in [1, 3, 8]. A subjective trust evaluation framework is to overcome these vulnerabilities, taking subjective consciousness of users into consideration. Even though the reputation value of a node is low, due to subjective willingness, another node may select it for routing or message relaying. Although some nodes have high reputation value, due to heavy networking load, low battery power or other reasons, sometimes we need to choose other nodes. In this case, more evaluation factors should be involved in the trust evaluation in MANETs.

To describe the trust in a node accurately, at least these three important parameters such as trust value, reputation value and confidence value should be considered. Trust value corresponds to the degree of trust to a particular behavior of other nodes. The value of reputation corresponds to the value of public confidence in the node. Confidence value is another essential parameter that characterizes the statistical reliability of the computed trust value. If no confidence value is included in the trust evaluation, obviously the computed trust is untrustworthy because we are not sure whether enough observations have been collected. For reputation-based trust models in [1,8], confidence value is not involved in trust opinion formation, which appears to be a

problem. It makes the evaluated trust value skeptical to some extent.

Liu and Li proposed a reputation-based trust model, which can discover and prevent selfish behaviors by combining familiarity values with subjective opinions. This work accumulates subjective opinions from their common neighbors. The reputation computation results could be affected seriously by the opinions with a low uncertainty [11], which helps to recognize selfish nodes so that the convergence time for isolating selfish nodes is decreased. The simulation results show that the model is better than that of purely subjective-logic-based trust model, and achieves a 25% improvement in the convergence time of selfish nodes detection in the network, which indicate that it satisfies the criterion of trustworthiness and uniformity. It can aware the neighbor nodes' familiarity, thus it satisfies adaptability. In this work, users can configure the weight of the factor of recommend nodes' opinions, thus it satisfies usability. The focus in this work is to discover and prevent selfish behaviors by combining familiarity values with subjective opinions, however privacy preserving has not been mentioned, so the criterion of privacy is marked"—". Since a node could obtain information from neighbor nodes and there's no any privacy preservation considered, node privacy leakage could be a potential security problem. It indeed can decrease the convergence time for isolating selfish nodes, so the criterion of accuracy is satisfied. It can continuously manage the dynamic trust relationship and recommendation, so it satisfies efficiency. It analyzed and simulated in three different scenarios, generality is satisfied, and considered local trust, recommend opinion and weight, other factors were not mentioned. Another problem is it lacks a metric that can model the drastic reduction of trust value when one node behaves maliciously and its slow increase when the node tries to rebuild its trust.

Djatmiko presented a framework for trust evaluation including generation, distribution and discovery of trust evidences without simulation in [6], therefore it may satisfies trustworthiness, accuracy and efficiency, but not tested and verified. This scheme does not integrate the confidence valuation of trust evidence to real-time, policy-compliance checking, thus it does not satisfy and adaptability. To prevent malicious nodes from leaking trust evidence of others, the policy require adequate, independent pieces of evidence before starting evaluation process, so it satisfies the requirement of privacy preserving. The issue of user designing the trust solution is not mentioned, so this model didn't satisfy usability. In this work it has taken into consideration subjective belief, confidence, therefore uniformity is satisfied. It listed some application scenarios for this model like military, therefore generality is satisfied. But one problem is that the trust evidence is not real time information, the accuracy of trust evaluation is hard to be ensured.

According to [16], Garg and Misra developed an opinion based trust evaluation model, which is responsible for evaluating a node behavior and categorizing it as well-behaving, misbehaving or suspicious nodes. The simulation result shows that as the presence of malicious nodes increases, the proposed trust evaluation model works well to identify and isolate the malicious nodes and improves throughput through providing secure routing path free of malicious nodes. With the percentage of malicious nodes increasing from 0 to 40%, the throughput is significantly decreased in DSR. But the impact of this decline is obviously less on the proposed this opinion based trust evaluation model, compared with DSR. Therefore, it satisfies trustworthiness and accuracy. This model can aware different kinds of malicious behaviors and opinion of other nodes as described above, so the criterion adaptability is satisfied. And it can dynamically detect malicious nodes and category them, so it satisfies efficiency. A equation was proposed to the weighted trust which can relate to trust value to compute the opinion weight, which indicate it satisfies uniformity. The trust factors it focuses on include only packet drop rate , packet modification, subjective opinion and other malicious behaviors, thus it satisfies comprehension. In this work, the issues of trust solution designed by user and different scenarios were not take in to consideration, therefore usability and generality both are marked as "—". The method requires opinions of other nodes before the process to isolate misbehaving node, which means it can master many others' information, but privacy preserving was not considered in [16]. What's more, there are some other problems in this work, trust decay over time and trust acquirement through malicious behavior, were not solved. In addition, selfish or misbehaving nodes may at first agree to help other nodes to forward packets but later for some reason silently drop packets to save their resources, which is a knotty problem not solved.

3.2 Policy-Based Trust Models

Policy-based trust model is based on objective trust schemes such as logical policy and verifiable attributes encoded in signed credentials for access control of other nodes to the resources. Such a policy-based trust model usually makes a binary decision, such as whether the requester is credible or not, and whether the access request is permitted. Because of this nature of decision making, policy-based trust models have less flexibility, unlike reputation-based trust models.

In this subsection, we classify policy-based trust models according to the generation of final trust value into three types as described below. According to the classified types, we compare and analyze existing general models and schemes for trust (or reputation) evaluation.

3.2.1 Trust Models Using Weight-based Policy

As for the calculation of trust value, most of the proposed schemes apply a weighted sum of trust evidences. Therefore, weights should be perfectly adjusted in order that a more important parameter is tied with a high weight, for example, direct trust should have a higher weight than indirect trust.

Grey theory is a good method using data mining to handle the uncertainty among small samples, incomplete information, and lack of experiences [21]. A MANET system can be considered as a grey system GM(1,1) as described in [21]. Based on the theories of fuzzy recognition with feedback, SCGM(1,1) model and Markov chain, Zhang F. et. al. proposed a mode of predicting. In this work, the analysis and the trust assessment example shows that the models can be applied to the trust evaluation in different application scenarios, so it satisfies generality. It is suitable for computer calculating automatically and dynamically; therefore it meets the criterion of efficiency in trust evaluation in MANETs environment. The simulation results show a lower packet dropping rate, high transmission speed and high fitting value, so it correspondingly satisfies trustworthiness and accuracy. This work computes a combined value of multi-dimensional attributes, thus comprehension is satisfied. It combines the weight of the subjective view and the objective trust evidence to calculate the trust value, so it satisfies uniformity. A optimized fuzzy recognition method was used in this model to aware trust factors, which indicates that it satisfies adaptability. Because it does not

consider that privacy preserving and user designing or configuring the trust solution, thus usability and privacy both are marked as"—". However GM(1,1) has a disadvantage that it does not work for random fluctuations of these indicators. According to the analysis on the trust evaluation model SCGM(1,1) in MANETs, it didn't achieve drastic deduction on trust values when one node behave maliciously, but slow increase of the trust values when nodes rebuild trust.

In [14], Omar, Challal, and Bouabdallah proposed a fully distributed trust model based on trust graph for MANETs, which enables terminals to conduct the operations of generation, storage and distribution of the public key certificates with no central-node or authenticated party. In this work, comparing with two PGP-based systems, the developed system using a replica mechanism to get a maximum of partial certificates and to eliminate a maximum of fake certificates, so that the success rate is kept high. This model achieves a good performance in certification rate and detection rate with compare to two PGP-based systems, which indicate that it satisfies efficiency and trustworthiness. The topology dynamically change and historical trust have not simulated in this work, context-aware not being considered, so adaptability is marked as "—", and it does not support user' design of trust policy, so usability is not supported. The proposal itself is based on encryption and certification, which could efficiently prevent from privacy leak, thus the criterion of privacy and accuracy are satisfied. What's more, uniformity was not supported as it has not related the weight of voting or subjective view to trust value. Different application scenarios have not yet been mentioned and tested in this paper, therefore generality is "—".

The measurement and calculation of trust to secure interactions between mobile nodes in MANETs is crucial for the development of trust mechanisms. Luo, Liu, and Fan developed a trust model using a fuzzy recommendation similarity (RFSTrust) for MANETs in order to secure the network and improve the performance of MANETs trust model [12]. Theoretical analysis and simulation results show that RFSTrust is still robust in a general condition, in which selfish nodes cooperatively attempt to intently subvert the network, terminal to terminal packet delivery very quickly, and the average energy consumption decreased, which shows it satisfies accuracy. Only one type of situation was considered when selfish nodes attack in this work, therefore, trustworthiness is partially satisfied. The trust factors include many but incomplete, such as opinions, recommend honesty, past experience, so comprehension is satisfied partially. The proposed scheme could be employed to enforce cooperation among nodes and counter with non-cooperative nodes in a MANET environment. Nevertheless, the work only tested the performance of selfish nodes, it should measure the trust value and performance of all neighbor nodes to select the most trusted route, it cannot achieve context-awareness, and the criterion adaptability is not satisfied. The model could support users' configuration of the weight of direct rating, negative behavior, uncertainty behavior, the threshold value of the data forwarding times and recommending times, thus it satisfies usability. The scheme focuses on packet forwarding and average energy economic consumption, privacy preservation is not mentioned. What's more, the problem is that it haven't measure all kinds of factors that can influence trust and simulate them in different dynamic scenarios, thus efficiency is not satisfied.

Hu and Perrig proposed a secure on-demand routing protocol for ad hoc networks called Ariadne [7] that can prevent attackers or malicious nodes from manipulating the information of trusted routes comprised of trusted nodes. It can also prevent many types of attacks, including DOS attacks. Therefore, it satisfies trustworthiness. Ariadne can operate on-demand and discover routes between terminals dynamically, so efficiency is satisfied. Because the proposed protocol is less efficient than the highly optimized version of DSR in evaluating and analyzing the effect of the optimization and security, so it does not satisfy accuracy. This model can aware Scenario parameters, DSR parameters, TESLA parameters, thus adaptability is satisfied, and those are all trust factors, thus it satisfies comprehension. In this scheme, users cannot set trust policies, thus it does not satisfy usability. Privacy preservation in different application scenarios was not considered. And it didn't support users' subjective opinion or voting, so it did not conform the criterion privacy. One problem is that there's no such fine-grained path control in existing distance vector routing schemes, which makes this trust model more challenging to ensure security.

3.2.2 Trust Models Using Threshold Policy

The main concern of trust models using threshold policy for trust decision making is to filter out the untrustworthy nodes, or more precisely speaking, whose trust values are below a certain threshold. This method is the easiest and mostly adopted with regard to making use of the trust values of the nodes.

In [18], Venkataraman, Pushpalatha, and Rao presented a trust model that incorporated a Vector Auto Regressive (VAR) trust model into an active and passive MANET routing protocol. In [18], the picture of throughput of the network in fig. 6 shows AODV with VAR is able to identify the adversary nodes. Therefore it satisfies accuracy. This model can detect flooding attacks and content modification attacks, other kinds of attacks were not tested in the simulation, so it satisfies trustworthiness partially. The equation store the historical information related to trust in a matrix, it can aware historical trust and meets the criteria adaptability. The trust model collects plenty of information by the method that neighbor nodes can be judged for its honesty in communication participation, data forwarding. Hence, they used a regression model where each trust factor aspect of neighbor nodes is calculated as a vector item. Therefore the criterion comprehension is satisfied. Since the focus of this work is selection of route based on trust evaluation, privacy preserving were not supported, the privacy-preserving criterion is not supported. Moreover, related subjective opinion and users' voting with trust weight should be ensured, but they have not taken into consideration, therefore the criterion uniformity is marked as "N". By comparing the throughput between VAR and traditional OLSR, the trust of former is almost 3.5 times of the latter, the route selection performance was improved. Therefore the criterion efficiency is satisfied. Different application scenarios were not mentioned in this work.

In [10], Li .et al. proposed a trust model to evaluate neighbors' behaviors based on packet forwarding ratio and a multi-path reactive routing protocol for MANETs, termed as AOTDV. Through calculating hop counts and trust value, this protocol can discover multiple trusted paths evaluated. In this work, the simulation result shows that, with the nodes speed increasing, the delivery ratio of AOTDV swings, but the delivery ratios of AODV and AOMDV decrease, so it meets the requirement of accuracy. This model can aware historical trust and evaluate current value, so it satisfies adaptability. Multiple paths can also be used to balance load by forwarding data packets on multiple paths simultaneously. The routing overhead of AOTDV and

AOMTV still kept relatively a low level while that of AODV is higher because of the multi-path feature. In the condition that the speed is above 5 m/s, AOTDV is lower than AOMDV with regard to average latency, which indicates that efficiency is satisfied. What's more, trustworthiness is partially satisfied because the attacks it can prevent include many, such as modification attacks, gray hole attacks or black hole attacks, but incomplete. But, this scheme should, to a large extent, increase the probability of attacks in the simulation, to test the performance when it exposed to saturation attacks, which proofs trustworthiness is partially satisfied. Even though it can improve the performance trust route selection, it didn't support subjective opinion or voting, so it did not conform the privacy preserving when the nodes all can obtain neighbor nodes' information. Other kinds of scenarios were not considered and tested in this work, thus the criterion generality has not yet been considered.

Xu et al. proposed a policy enforcing mechanism based on Satem [20], which is a kernel-level trusted execution monitor based on the theories of trusted platform module. Using the proposed mechanism, each application scenario is assigned with an associated policy. Meanwhile, users can set their trust solutions. Thus, it satisfies usability. Different scenarios were tested in this work, including random waypoint scenarios, walking scenarios and vehicular network scenarios. Therefore it supports generality. In fact, this scheme is susceptible to numbers of attacks due to bugs in the module of boot loader, BIOS, and TPM, so it does not satisfy trustworthiness. The dynamic root of trust feature of new processors may mitigate these vulnerabilities. Through the application execution context, the trusted node could verify the integrity of the service code loaded dynamically, which indicate it satisfies the criterion adaptability. Only the nodes whose trust value above a certain value are allowed to join the trusted route, the more number of hops a node is away from the network originator, the longer it takes for it to join the tier, and the overhead is larger. Comparing with other trust models, the merged has a lower overhead rate and higher service complete ratio, thus it satisfies efficiency. However, the trust factors only include software malicious code and integrity of the system, which indicates comprehension not satisfied. In this work, the impact of users' subjective opinion to trust value and privacy preserving were not taken into consideration, therefore privacy and uniformity are marked as "—". The results demonstrated the mechanism has the advantages including feasibility and low overhead, and it ensures that a protected service cannot load untrusted codes. But one problem is that it is unable to tackle attacks, like buffer overflow, that can cause the protected service to run arbitrary code without changing its disk image.

Roughly, in the threshold-based trust models, when one neighbor's trust value is lower than a threshold, it will be regarded as a malicious node, and then removed from the neighbor set, finally added into the black list. That is, the whole network will ultimately deny it. The proposed trust models based on threshold policy have different focuses, some of them did not consider trust factors comprehensively, and some of them did not employ an efficient metric for trust evaluation. Each of above model has some disadvantages as we have described and analyzed. Most schemes do not consider privacy preservation, and the trust factors considered are not complete. Only few models are compatible or applicable in different scenarios. Moreover, trust re-establishment was not considered and supported.

3.2.3 Trust Models Using Load-Balancing Policy

Because of the open natures of MANETs, the selection of trust route is an important challenge, especially when the resources (e.g., battery and bandwidth) of the mobile devices are limited and should not be wasted on erroneous or malicious contents. Trust evaluation should consider load balancing, because the volume and flow of access of the most trusted nodes will grow rapidly in no load-balancing-based trust models since all nodes will select the most trusted nodes. Obviously, many types of Denial-of-Service attacks may be launched to one or more nodes if not considering load balancing. A trust model should prevent overuse of a single node's resources with regard to accurately choosing trustworthy nodes.

Due to that a node usually request the trust and reputation information before communication start, trust approaches with poor trust and reputation acquisition latency are unacceptable in strict real-time required environment, such as battleground and emergency rescue. So, Boukerch, Xu and El-Khatib presented a trust and reputation evaluation model named ATRM [2] aiming to manage trust and reputation with a minimal extra messages overhead and time delay overhead. A node store and manage trust and reputation information on the local agent. This brings with a benefit that the nodes themselves can provide their own trust and reputation information rather than in a way of network-wide flooding and acquisition-latency. The proposed ATRM can aware an arbitrary context in the simulation, which shows a good performance in ATRM packet transactions and average acquisition delay, therefore the criterion adaptability is satisfied. It can prevent from modification attacks and can be resilient against attacks of defamation and collusion as described in the result, but other attacks were not focused on, so it satisfies trustworthiness partially. However, trust is not only related to the node itself, it should receive trust evidences or opinions from other nodes. This model did not completely consider trust factors, such as confidence were not included, therefore, it satisfies comprehension partially. The model was tested and analyzed in a fixed environment, rather than in an environment with dynamic changes, thus, it didn't conform the criterion generality. Since the simulation was conducted in a dynamic environment, the result showed a good performance in terms of acquisition delay and delivery ratio, so efficiency is satisfied. But accuracy is not considered, because it has not simulated the dynamic trust relationship. Moreover, it does not support subjective view or voting, therefore uniformity is not satisfied. Privacy preserving is also an important and crucial issue, which is not mentioned and considered in this work and should be solved.

A trust and probabilistic node selection mechanism for content distribution in MANETs was proposed by Djatmiko et al in [5]. Load balancing was achieved by selecting randomly a node from a set of trusted nodes. The proposal, not only considered the trustworthiness of the terminals, but also ensured the participants equally share the routing load, so as to conserve resources in the network and prevent from overusing resources of a single node with regard to accurately choosing trusted nodes and provide required contents. This trust model evaluate trust according to interaction data, historical trust value, context, and opinions from other nodes, so it considered almost all trust aspects and can dynamically aware the context, so the criterion comprehension and adaptability are satisfied. As is shown in the simulation result, the mean absolute deviation demonstrates an accurate trust calculation (shown as best trust cases) and more reliable node selection, which indicates accuracy and efficiency are satisfied.

Although it considered the opinion of other nodes, it did not relate the opinion weight to the trust value, uniformity is not satisfied. This work concerned resource consumption in trust evaluation by treating node resources as one impact factor in trust evaluation, and has not consider the issue of policy setting by users, so the criterion usability is marked as "—". It can be observed in experiment result that the effect of noisy behavior is marginally reduced when using this probabilistic node selection mechanism, and it can prevent from DOS attacks by load balancing, so trustworthiness is satisfied partially. However, the issues like privacy preservation, which has not been considered, would become important since nodes in the network can master node information about its resources.

In [17], Seredynski and Aggoune proposed a trust evaluation model based on collaborative sanction, and showed a significant improvement in performance of added throughput and average throughput. Through collaborative sanctioning, MANET could benefit from the extension of a reputation system with a trust system. This work concerns on throughput based on trust evaluation and has not consider the potential attacks. Therefore it does not satisfy trustworthiness. It collects first-hand (personal and general) evidence and second-hand (personal and general), many but incomplete, thus comprehension is partially satisfied. The result of the simulation indicates that the trust rating and reputation rating is acceptable, so it satisfies accuracy. The issue of using weighted recommend opinion and different application scenarios were not considered, so uniformity and generality both are "—". Trust can be classified into provision trust, access trust, delegation trust, identity trust and context trust as described in [17], and this work only deals with provision trust and context trust is neglected. Therefore, it does not satisfy adaptability. Privacy preserving is not supported in this model, how to prevent trust evaluation from potential attacks and privacy leakage while sharing of information for trust justification without a rigorous authentication scheme is still a problem.

In terms of DOS attacks, the attacker aims to make victim nodes or even the whole network crashed through intruding the target with a large number of accesses. To solve this vulnerability existing in MANETs, Li, Li, and Kato designed a robust and attack-resistant framework, which is called the Objective Trust Management Framework (OTMF) with the idea of load balancing [9]. According to the simulation result about, trustworthiness obtained by the OTMF compared with other reputation-based frameworks, it performs better on trustworthiness for honest nodes but lower for attackers, which indicates that it satisfies efficiency and accuracy. This framework offers a good way to prevent the following attacks: selective misbehavior, bad mouthing and conflicting behavior, other attacks not being considered, therefore it satisfies trustworthiness partially. It considered subjective view (confidence value) of other nodes and combined it with second-hand information, trust value, and recommend value, so it satisfies uniformity and comprehension. The framework cannot measure trust value according to the context, thus adaptability is not satisfied. Privacy preserving is not the focus of this work. Different application scenarios were not tested and verified.

A trusted model based on the dynamic trust mechanism by extending the dynamic source routing protocol was proposed in [15]. If a node's trust value is high, but its load performance is relatively poor, in this case, this model applies load balancing by recommending other routes to a route requester. This mechanism accesses recommendation trust to prevent dishonest recommendations and associate trust levels with network nodes in order to compute trusted routes. In this model, a dynamic trust mechanism was applied, rather than using a hard security mechanism, which shows a good performance in terms of RREP delivery, route selection and time-delay, according to the simulation result. Consequently, it satisfies the criterion of accuracy and efficiency. The trust factors it considered includes direct trust and reputation trust, but indirect trust and confidence not included, thus comprehension is not satisfied. Moreover, it does not support voting according to trust value. However, they did not take into consideration several issues, as listed in the following. It didn't consider that how to detect and defend internal attacks and external attacks against routing protocols, therefore it does not meet the requirements of trustworthiness. And how to quantify and evaluate the trade off between the trustworthiness and the performance it lacks a concrete policy to solve it. What's more, the proposed trust model can't evaluate trust according to network context and adapt to its changes. Thus, adaptability is not satisfied. In view of the different application scenarios, which is this work not considered, the deployment of framework is questionable.

According to the above review of the existing work and comparison of their trust evaluation model by referring to the above described nine criteria, the analysis result is as shown in Table 1.

Table 1. Comparison of Existing Work Based on The Proposed Review Criteria

Paper	T	Ad	Us	P	Ac	E	Un	C	G
[1]	P	Y	—	N	Y	Y	N	Y	—
[2]	P	Y	—	—	—	Y	N	P	N
[3]	P	Y	N	—	Y	—	Y	Y	—
[4]	P	Y	Y	—	Y	Y	—	N	—
[5]	P	Y	—	—	Y	Y	N	Y	Y
[6]	—	N	—	Y	—	—	N	Y	Y
[7]	Y	Y	N	N	N	Y	—	Y	—
[8]	Y	Y	—	—	Y	Y	N	N	—
[9]	P	—	—	—	Y	—	Y	Y	—
[10]	P	Y	—	N	Y	Y	—	P	—
[11]	Y	Y	—	—	Y	—	Y	N	—
[12]	P	N	Y	—	Y	N	—	P	—
[14]	Y	—	N	Y	Y	Y	N	Y	—
[15]	N	N	—	—	Y	Y	N	N	—
[16]	Y	Y	—	—	Y	Y	Y	Y	—
[17]	N	—	—	N	Y	—	—	P	—
[18]	P	Y	—	N	Y	Y	N	Y	—
[20]	N	Y	Y	—	—	Y	—	N	Y
[21]	P	Y	—	—	Y	Y	Y	P	Y

Y: supported; N: not supported; P: partially supported —: not mentioned or considered.

4. PROBLEMS OF CURRENT RESEARCH AND FUTURE RESEARCH TRENDS

4.1 Problems and Open Issues

Based on the literature review and evaluation according to the proposed criteria, we summarize the open problems existing in the proposed trust models. On the basis of the above analysis and comparison, we find that although much research has been conducted, still many problems exist. Most trust models we analyzed above didn't take into consideration and handle perfectly these problems in order to satisfy all specified criteria. Generally the following issues about trust evaluation in MANET should be considered thoroughly.

Based on the above review, we found some work evaluated trust from one or two angles. Most current schemes proposed didn't comprehensively consider multiple-dimensional trust. As described, considering all of the factors could introduce high computation, process and communication overhead. Only a few trust models considered different application scenarios and meet the generality [6, 20, 21]. All of the proposed trust models neglected or cannot handle perfectly the issue of privacy preservation in MANETs. Most of proposed trust models cannot evaluate trust according to the changeable mission contexts and requirements, none existing work listed above offered a context-aware trust model that holistically and flexibly considers all trust factors in MANETs. Moreover, the metrics proposed in these trust models were not very accurate. Besides, another drawback of the existing work is that most trust models treated node feedback equally, which impacts the accuracy of trust evaluation. In general, a uniform model that considers node users subjective voting with trusted credibility for trust evaluation lacks in existing studies.

Generally the following issues about trust evaluation in MANET should be considered thoroughly.

1) The issue of privacy preservation in MANET has not been solved perfectly. So far, few schemes about privacy preserving in MANETs were proposed. Unauthorized parties should not access various user information, e.g., behaviors, resources, locations and identities. It still lacks a scheme to ensure the performance of MANET services and at the same time preserve the privacy of users. However, privacy-preserving schemes usually have seldom been concentrated.

2) Because the MANET has the features of mobility and complexity, existing trust evaluation models in MANETs are cannot support context-awareness. Since MANETs have different mission contexts and requirements in terms of trust level and performance. A number of proposed trust models cannot adapt to these changes.

3) It lacks a metric or algorithm that can model the drastic reduction of trust value when one node behaves maliciously and its slow increase when the node tries to rebuild its trust. Thus the trust evaluation can resist some attacks like on-off behavior and conflict behavior attacks effectively.

4) Some models' drawback is that it treated equally on node feedback and score. Some feedback information from malicious nodes may damage the accuracy of trust evaluation.

4.2 Future Research Trends

All above challenges and open issues motivate future research. In the future, other types of nodes attacks and possible impacts trust model could be raised. Investigating adaptability, usability, privacy, and uniformity in the trust evaluation offers additions rooms for further improvements for achieving more advanced trust models for MANETs. Herein, we further suggest a number of promising research directions about trust evaluation in MANETs as below.

a) **Privacy preservation.** Node privacy should be well preserved in MANETs. Nowadays, node users pay more attention to their personal privacy especially when they communicate in MANETs, because the other side of the communication is probably a stranger in many MANET application scenarios. Therefore, designing effective personalized privacy protection schemes that can assure the user privacy when user data are collected for trusted evaluation becomes particularly important.

b) **Context-awareness.** Trust models should be situation specific with context-awareness. Since the MANET has the features of mobility and complexity. So, MANET trust evaluation should sense mission contexts and requirements in terms of trust level and system performance. Depending on the required levels of security, performance and/or reliability, a different level of trust with different considering factors and evaluation algorithms can be adopted adaptively.

c) **Comprehensive model.** A comprehensive trust evaluation model should be proposed that reflect trust changes dynamically based on node behaviors and can consider all trust influence factors in an adaptive measure. This is an indispensable and important issue in the trust evaluation in MANETs.

d) **Uniform model to judge node subjective feedback and scores.** As different nodes could provide their feedback based on different standards, and reputation and trustworthiness of different nodes are different, we should provide a uniform method to aggregate feedback and scores collected from different nodes in the process of trust evaluation.

5. CONCLUSIONS

In this paper, we introduced the basic knowledge of trust and MANETs, and reviewed recent work related to trust evaluation and performed a serious survey on the trust evaluation of MANETs based on nine proposed criteria. Through study and analysis, we found there are still a number of drawbacks in these works and presented several open issues regarding trust evaluation research in MANETs. We suggested future research focuses by directing a number of research trends. We found that significant efforts are needed in order to solve those problems and overcome challenges for enhancing trust collaboration in MANETs.

6. ACKNOWLEDGMENTS

This work is sponsored by the NSFC (grant U1536202), the 111 project (grant B08038), the PhD grant of the Chinese Educational Ministry (grant JY0300130104), the Natural Science Basic Research Plan in Shaanxi Province of China (Program No. 2016ZDJC-06), and Aalto University.

7. REFERENCES

[1] Banerjee, A., Neogy, S. and Chowdhury, C. 2012. Reputation Based Trust Management System for MANET. In *International Conference on Emerging Applications of Information Technology* (Kolkata, India, November 30-December 1, 2012). EAIT'12. IEEE, Washington D.C. 376-381. DOI=http://dx.doi.org/10.1109/EAIT.2012.6407975.

[2] Boukerche, A. Xu, L. and El-Khatib, K. 2007. Trust-based security for wireless ad hoc and sensor networks. *J. Comput.*

Commun. 30 (Apr. 2007), 2413-2427, DOI=http://dx.doi.org/10.1016/j.comcom.2007.04.022.

[3] Boukerche, A. and Ren, Y. 2008. A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks. In *Proceedings of the Fifth ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks* (Dublin, Ireland, March 22 - 26, 2014). PE-WASUN '08. ACM, New York, NY, 27–28. DOI=http://dx.doi.org/10.1145/1454609.1454628.

[4] Chen, H. and Fu, Z. 2011. A Novel Trust Routing Scheme Based on Node Behavior Evaluation for Mobile Ad Hoc NETWORKS. *J. Intell. Auto. Soft. Comp.* 17 (Mar. 2013), 1063-1074. DOI=http://dx.doi.org/10.1080/10798587.2011.10643211.

[5] Djatmiko, M., Boreli, R., Seneviratne, A. and Ries, S. 2013. Resources-aware trusted node selection for content distribution in mobile ad hoc networks. *J. Mob. Com. Com. Inf.* 19, 5 (Sep. 2012), 843-856. DOI=http://dx.doi.org/10.1007/s11276-012-0505-5.

[6] Eschenauer, L., Gligor,V. D. and Baras, J. 2004. On trust establishment in mobile ad-hoc networks. In *Proceedings of the 10th International Workshop* (Cambridge, UK, April 17-19, 2002). LNCS'02. Springer, Berlin, H. Ber, 47-66. DOI=http://dx.doi.org/10.1007/978-3-540-39871-4_6.

[7] Hu, Y.C. and Perrig, A. and Johnson, D. B. 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. *J. Wireless Networks.*11 (Jan. 2005), 21-38. DOI=http://dx.doi.org/10.1007/s11276-004-4744-y.

[8] Kpodjedo, S., Pierre, S. and Polytechnique, É. 2008. Reputation based trust management using TCG in Mobile Ad-Hoc networks (RTA). In *Proceedings of the 33rd Annual IEEE Conference on Local Computer Networks* (Montreal, Que, October 14-17, 2008). LCN '08. IEEE, Washington, DC, 518 - 519. DOI= http://dx.doi.org/10.1109/LCN.2008.4664218.

[9] Li, J., Li, R. and Kato, J. 2008. Future trust management framework for mobile ad hoc networks. *J. Commu. Magaz.* 4 (Apr. 2008), 108-114. DOI=http://dx.doi.org/10.1109/MCOM.2008.4481349.

[10] Jia, L., X., Wang, L. G. and Wang, H. Y. 2009. Trust-based on-demand multipath routing in mobile ad hoc networks. *J. IET. Inform. Secu.* 4 (Aug. 2009), 212-232. DOI=http://dx.doi.org/10.1049/iet-ifs.2009.0140.

[11] Liu, Y., Li, K., Zhang, J. Y., and Qu, W., 2010. A novel reputation computation model based on subjective logic for mobile ad hoc networks. In *Third International Conference on Network and System Security* (Gold Coast, QLD, October 19-21, 2009). NSS'09. IEEE, Washington, DC, 294 - 301. DOI=http://dx.doi.org/10.1109/NSS.2009.68

[12] Luo, J., Liu, X., and Fan, M., 2009. A trust model model based on fuzzy recommendation for modile ad-hoc networks. *J. Network.Comp.App.* 28 (Sep. 2009), 2396-2407. DOI=http://dx.doi.org/10.1016/j.comnet.2009.04.008.

[13] Govindan, K., and Mohapatra, P. 2008. Trust Computations and Trust Dynamics in Mobile Ad hoc Networks: A Survey. *J. Comp. Security.* 14 (May. 2011), 279-298. DOI=http://dx.doi.org/10.1109/SURV.2011.042711.00083.

[14] Omar, M., Challal, Y., and Bouabdallah, A. 2009. Reliable and fully distributed trust model for mobile ad hoc networks. *J.Com. Sec*. 28 (Dec. 2008), 199-214 .DOI=http://dx.doi.org/10.1016/j.cose.2008.11.009.

[15] Peng, S., Jia, W., Wang, G., Wu, J. and Guo, M. 2010. Trusted Routing Based on Dynamic Trust Mechanism in Mobile Ad-Hoc Networks. *IEICE Trans. Inf. & Syst. 93, 5* (Mar. 2010) 510-517. DOI=http://dx.doi.org/10.1587/transinf.E93.D.510.

[16] Garg, P., K. and Misra, M. 2011. Opinion Based Trust Evaluation Model in MANETs. In *Proceedings of the 4th International Conference on Communications in Computer and Information Science* (Noida, India, August 8-10, 2011). CCSIS'12. Spring, Berlin, H. Ber, 301-312. DOI=http://dx.doi.org/10.1007/978-3-642-22606-9_32.

[17] Seredynski, M., Aggoune, R., Szczypiorski, K. and D., Khadraoui. 2013. Performance Evaluation of Trust-based Collaborative Sanctioning in MANETs. In *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (Melbourne, VIC, July, 16-18, 2013). TrustCom'12. IEEE, Washington, DC, 81 - 88. DOI=http://dx.doi.org/10.1109/TrustCom.2013.14.

[18] Venkataraman, R., Pushpalatha, M. and Rao, T., R. 2012. Regression-based trust model for mobile ad hoc networks. *J. Info. Sec.* 6 (Sept. 2012).131-140. DOI=http://dx.doi.org/10.1049/iet-ifs.2011.0234.

[19] Wang, K., Wu, M. and Shen, S. 2008. A trust evaluation method for node cooperation in mobile Ad Hoc. In *Proceedings of the Fifth International Conference on Information Technology* (Las Vegas, NV, April 7-9, 2008). ITNG'08. IEEE, Washington DC, 1000 - 1005. DOI=http://dx.doi.org/10.1109/ITNG.2008.43

[20] Xu, G., Borcea, C. and Iftode, L. 2011. A Policy Enforcing Mechanism for Trusted Ad Hoc Networks. *J. Depen. Sec. Comp.* 8 (May, 2011), 321-336. DOI=http://dx.doi.org/10.1109/TDSC.2010.11.

[21] Zhang, F., Jia, Z., Xia, H., Li, X., and Edwin, H. M. S. 2012. Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM (1, 1) model. *J. Comp. Comm.* 35 (Mar, 2012) 589-596, DOI=http://dx.doi.org/10.1016/j.comcom.2011.10.007.