future internet

MDPI

Article

An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs

Muhammad Salman Pathan *, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon and Muhammad Iftikhar Hussain

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China; znf@bjut.edu.cn (N.Z.); jhe@bjut.edu.cn (J.H.); zulfiqar@emails.bjut.edu.cn (Z.A.Z.); kasim@emails.bjut.edu.cn (M.Q.M.); hussain@emails.bjut.edu.cn (M.I.H.)

* Correspondence: salman@emails.bjut.edu.cn; Tel.: +86-130-2108-3511

Received: 15 November 2017; Accepted: 23 January 2018; Published: 5 February 2018

Abstract: Due to the dynamism of topology, sharing of bandwidth and constraint of resources in wireless nodes, the provision of quality of service (QoS) for routing in mobile ad hoc networks (MANETs) presents a great challenge. Security is another crucial aspect of providing QoS since the existence of malicious nodes present all kinds of threats to MANETs. Although a number of mechanisms have been proposed for protecting MANETs, most of the solutions are only effective for a particular kind of attacks or provide security at the cost of sacrificing QoS. In this paper, we propose a trust-based secure QoS routing scheme by combining social and QoS trust. The primary approach of the proposed scheme relies on mitigating nodes that exhibit various packet forwarding misbehavior and on discovering the path that ensures reliable communication through the trust mechanism. The scheme would select the best forwarding node based on packet forwarding behavior as well as capability in terms of QoS parameters, such as residual energy, channel quality, link quality, etc. We will present an adversary model for packet dropping attack against which we evaluate the proposed scheme. Simulation experiment using Network Simulator-2 (NS2) and under various network conditions show that mixing social and QoS trust parameters can greatly improve security and quality of service routing in terms of overhead, packet delivery ratio and energy consumption.

Keywords: mobile ad hoc networks; QoS routing; packet-forwarding misbehavior; trust-based scheme

1. Introduction

Along with the widespread use of cheaper, smaller and more powerful wireless nodes over the past few years, mobile ad hoc networks (MANETs) have received much attention, making it one of the most promising areas of wireless network development [1,2]. MANET is a self-organizing, dynamic, infrastructure-less network consisting of a set of wireless nodes that communicate with one another over one or more connections or hops without the need of a central authority [3]. In a MANET, each and every node can function both as a terminal node and as a router, meaning that each node could generate its own traffic while receiving data packets from other nodes and forwarding them to the neighboring nodes. MANETs can be deployed quickly and easily, making them very suitable for applications such as environmental monitoring, military surveillance, disaster rescue, etc. [4,5].

Quality of Service (QoS) routing is a necessary function in MANETs. In addition to finding the routes from a source to a destination, QoS routing also needs to ensure end-to-end quality, usually in terms of bandwidth or delay [6]. A major challenge for MANETs is the design of a secure and efficient routing protocol that can also ensure the overall quality of service during the routing process as MANET nodes communicate with each other only when they are located within the communication range of each other. When the receiver is far away from the transmitter, i.e., the destination is out of the transmission range of the transmitter, the dynamic nature of MANETs makes it difficult to ensure QoS

since the node-to-node channel and link quality changes dynamically which may result infrequent link failures and cause nodes to make connections with other nodes [7,8]. Another important issue in MANETs is security since malicious nodes can deliberately misbehave so that packet contents can be altered and packet routing to the desired destinations can be disrupted, lowering packet delivery ratio as well as reliability [9].

Security and trust are correlated with each other. In trust-based security, when trust level increases, so do the access privilege for security protection. In MANETs, trust can be defined based on "the closeness of the relationships between entities that participate in a protocol interaction". There are generally two types of trust: social trust and QoS trust with social trust being obtained based on social relationships, e.g., friendship, honesty, privacy and intimacy while QoS trust being obtained based on competency, reliability, experience, number of packets forwarded, etc. [10]. There have already been some proposals for securing the process of routing in MANETs. Although cryptographic techniques have been widely used in routing to protect routing information from being tinkered by the adversary, such an approach may not be practical for real MANETs due to heavy computational overhead and lack of capability of spotting attacking nodes given the high mobility of MANETs where nodes continuously join and leave the networks [11]. Introducing "trust" into such a hostile environment can help nodes observe and predict the behavior of neighboring nodes in an efficient manner. The notion of trust is very useful in a highly dynamic environment where nodes need to depend upon each other to accomplish their common goals [12–14]. Trust-based routing has been considered as an effective measure to deal with security threats caused by malicious nodes through detecting and isolating untrusted nodes in MANETs [15,16].

In this paper, we propose a new and efficient trust-based secure QoS routing scheme (TSQRS) which combines social trust and QoS trust. The proposed scheme would selecta forwarding node by considering channel quality, link quality and residual energy in order to establish an optimal path in a very dynamic environment and detect intrusions by using the trust of neighboring nodes to mitigate threats by nodes misbehave in packet forwarding during the routing process. The proposed solution relies on the trust mechanism to provide reliable performance and secure links for data transmission and energy efficiency.

The remainder of this paper is organized as follows. Section 2 contains the review of some related work. Section 3 presents the proposed secure and QoS routing scheme after an adversary model is described and Section 4 contains some evaluation results to show the advantage of the proposed scheme over two other comparable schemes in terms of some important matrices. Finally, Section concludes this paper.

2. Related Work

Gite et al. proposed a new routing protocol by extending the conventional Ad Hoc On-Demand Distance Vector (AODV)called (TRUST_AODV) [7], incorporating a trust algorithm that detects misbehaving nodes within. An objective trust management framework is used in this approach for solving problems such as handling high node mobility, energy drain, and limited processing capabilities of network devices by establishing a network of nodes with an acceptable level of trust relationships among themselves. The weighted trust is computed for each node, by the proposed algorithm considering the packet delivery ratio, energy consumption rate and buffer length into account. The Overall performance of TRUST_AODV routing protocol indicates that it secures the MANET against potential packet drop attacks and denial-of-service (DoS) attacks.

Hinge et al. proposed an opinion based trust model which works on the basis of network properties [3]. In this solution, intermediate nodes' opinion trust is computed and based on suchan opinion trust value, the decision can be made regarding the use of a particular route for communication. Communication in MANETs has to be carried out through using intermediate nodes due to limited radio range. As a result, malicious nodes can join the network and harm the routing process. Thus, trust evaluation can yield two values at the minimum: negative and positive, in the process of finding

a trustworthy node. After deriving the trust values for all the nodes along a path, route discovery can be performed by taking the opinion of the neighboring nodes.

Koul et al. proposed a model that deploys security in MANETs while taking into consideration of QoS issues to some extent [8]. The proposed model is multilayered and composed of a set of modules, i.e., packet receiver, packet forwarder, QoS routing module (RM), system security module (SSM) and data security module (DSM). All the modules are needed in order to identify QoS parameters and to detect selfish and malicious nodes. Efficient and reliable communication is ensured by selecting an appropriate router between a source and a destination through trusted nodes in the place of eliminated nodes. Performance evaluation was done in an established secure environment to show the improvement over AODV for different QoS parameters for both single and multi-path environments.

Jhaveri et al. proposed a composite trust model which utilized both social and QoS trust components [11] to estimate the trust degree of nodes in which the ditch ratio was used as a social trust component. This ditch ratio parameter is valuable for knowing the behavior of nodes and to identify malicious nodes. In the paper, energy consumption was defined as an aspect of QoS by considering the ratio of packet drop of a specific node. Nodes with the lowest level of energy are considered as un-trusted nodes. The proposed scheme showed some enhancement in packet delivery ratio when compared to some other methods.

Sirisala et al. proposed a method to evaluate the trust value of a node based on its quality of service (QoS) parameters [15] where fuzzy rules were inferred based on network conditions. The proposed method used an algorithm based on Dynamic Adaptive Fuzzy Petri Net (DAFPN) with concurrent reasoning. DAFPN is an expert system to represent, capture and store fuzzy knowledge with the help of parameters such as threshold value, certainty factor and weight. The concurrent reasoning algorithm (CRA) is a matrix operation based algorithm, which can automate the procedure of DAFPN in which a MANET topology was modeled as a DAFPN to which FPN rules were applied. Route identification and recovery mechanisms with CRA used unicast and multicast methods and the proposed method included all the trustable intermediate nodes for routing.

Sethuraman et al. proposed an algorithm that used a management strategy for trust in a way in which packets can be sent securely through the network with a lower level of energy consumption [17]. The idea behind this approach is to assign a trust value to each node dynamically. Due to high mobility, there should be an integration of trust and energy consumption of every node. A new trust management model was thus proposed to enhance the routing security in the network in which both direct and indirect trust values were employed in trust calculation. Final trust value is derived based on direct trust value and indirect trust value. The Bayesian probability was also used as a technique for trust management to refine the calculation of trust. The algorithm forwards packets from a source to a destination through a reliable route that also consumes less energy.

Ahmed et al. presented an algorithm in which calculated trust values are used to identify malicious nodes [18]. True flooding approach was utilized to identify attacking nodes based on trust values. This work relied on identification and avoidance of malicious nodes as well as denial-of-service attacks on the network layer based on interaction history. A route discovery algorithm was developed to discover an efficient and secure path for data forwarding by using experimental grey wolf algorithm to validate network nodes. Enhanced multi-swarm optimization was also used to optimize the identified forwarding path. It was concluded that the proposed scheme was useful in terms of secure data dissemination in scalable MANET environments.

Kambourakis et al. proposed a public key management scheme using the trust graph model in this work [19]. Because of the frequent mobility of nodes, dynamic network topology, an absence of centralized administration and wireless connections, the traditional security solutions are not easily deployable in MANETs, and also the establishment of a Public Key Infrastructure (PKI) in such a dynamic network environment is a difficult task. In this regard, the authors designed a binary tree formation of the network's nodes, in order to build certificate chains between communicating nodes that are multi-hops away to avoid the clumsy problem of certificate chain discovery. Simulations of the

proposed scheme under different network scenarios demonstrate that it is very effective in terms of tree formation, certificate chain establishment between nodes and join and leave occurrences to make a balance between security and performance.

Rajkumar et al. proposed a Certificate distribution and a Trust based threshold revocation method. In this work, the authors developed a trust-based solution using an efficient mechanism for certificate revocation and validation by combining public key certificates [20], in order to enhance the security of the network by reducing the hazards from malicious nodes. Initially, the trust values were derived from the direct and indirect trust values and the secret key to all the nodes were distributed by a certificate authority. Followed by this, a trust based threshold revocation method is computed. Here the misbehaving nodes are eliminated.

Cho et al. proposed a composite trust-based public key management (CTPKM) approach with an idea of maximizing the performance of network while mitigating the vulnerabilities [21]. Based on the concept of trust, the proposed approach adopts fully distributed trust-based public key management based policy for MANETs using an easy security mechanism. This work aims to maximize performance by using trust-based approach, instead of using hard security parameters to remove security vulnerabilities. During the routing process, the nodes determine the trust of another node using a trust threshold. The results depict that CTPKM minimizes the risk at a large margin using an optimal trust threshold and maximizes the service availability with acceptable communication overhead acquired by trust and key management operations.

Going through all the previous work listed, we observed that integration of QoS trust and social trust could improve the performance of routing in MANETs. Considering these notes, we combine both the types of trust components in our work. We believe that the success rate of any security scheme largely depends upon the mode of operations of the adversaries, but it is to be noted that most of these schemes do not precisely describe the mode of operation for adversary models during route discovery phase and data transmission phase, to identify patterns followed by malicious nodes, while selecting trusted route for data transmission. We address this issue by introducing an efficient trust-based scheme which integrates attack pattern discovery to the trust mechanism by observing the packet forwarding behavior of nodes continuously. The scheme attempts to find attack patterns before a node launches packet dropping attack. The scheme identifies a distrusted neighbor during the trust update procedure and discovers an alternate route after discarding the untrustworthy route from the routing table which contains that malevolent node as next hop in a hostile setting.

3. Techniques and Methods

We describe the techniques and methods for secure and quality of service routing in MANETs in this section.

3.1. The Adversary Model

An adversary model for packet dropping attacks is used in this paper. In this adversary model (a type of gray-hole attack described as Attack1 in [22]), a malicious node continuously monitors the field value of received as well as overheard control packets, in order to keep track of the highest recorded value of the destination sequence number. During the routing process, the malicious node replies to an Route Request (RREQ) with the lowest hop count (which is 1) and the highest possible value of the destination sequence number. Even though the malicious node does not have a valid path, a genuine source node employing AODV protocol immediately can build a route through the adversary. The adversary then attempts to drop packets for the period of 50% of the total time. Packet dropping attacks happen at the time of routing data packets. The operations of the adversary model during route discovery phase and data transmission phase are presented in Figure 1.

Procedure 1: Actions by the malicious node after receiving RREQ from the source node
If (RREQ is not for me) **then**
Discard the received RREQ
//A random value between 1 to 10 add to RREQ DestSeqno
RREP packet Fill up with DestSeqno= RREQ DestSeqno + Random Number (1:10) and hop Count=1
Unicast the forged RREP on the reverse path to the source
Else
Fill up the RREP packet with own Seqno and Hop count=1
Discard the received RREQ
Unicast the genuine RREP on the reverse path to the source
END If

Procedure 2: Actions by the malicious node after receiving data packets from the source node
If (data packet is not for me) **then**
If (Current Time > time1&& Current Time <= time2) then//time2-time1=50% time period
The packets received from the source will be drop
Else
If a valid route is available the data packets will be forwarded
END If
Else
Receive the data packet for me
End If

Figure 1. Adversary model. Route Request (RREQ); Route Reply (RREP).

3.2. The QoS Parameters

The proposed routing scheme would select the next node for packet forwarding to the destination node based on the following three parameters: channel quality, link quality, and residual energy.

3.2.1. Channel Quality

In our scheme, channel quality means the availability of the channel during transmission. Measurement of interference in a channel can help utilize resources more effectively to ensure reliable communication. The use of channel quality metric also helps to reduce end-to-end delay through the allocation of on-the-fly radio resources. The capacity of a channel (H) is defined as the rate at which data can be reliably transmitted over the medium which can be calculated as follows:

$$H = G_t \times G_r \, (\lambda / 4\pi d)^2 \quad (1)$$

where G_t is the transmitter gain, G_r is the receiver gain, λ is the wavelength of the signal and d is the distance between the source and the destination.

3.2.2. Link Quality

In this paper, a new metric, i.e., link quality, is introduced which is measured as the length of time of the existence of a link between two nodes (link residual life). In our proposed scheme, we use the measurement value of the link quality to help reduce the route failure in a highly dynamic environment. Although the accurate depiction of wireless links in MANETs is a tedious task, link residual life can be relatively easily estimated based on the range of communication and a relative velocity between nodes. The time during which a link exists between nodes can be estimated as follows. First, we need to find the distance between nodes and its relative velocity. Considering a link between nodes A and B, let D be the distance between the two nodes. If ($x1$, $y1$) and ($x2$, $y2$) are the coordinates of nodes A and B, respectively, the distance can be calculated by using the following formula:

$$D = \sqrt{((x2 - x1)^2 + (y2 - y1))^2} \quad (2)$$

Let R be the communication range and $\Delta V = V_A - V_B$ be the relative velocity, the residual life of the link T is then $(R - D)/\Delta V$.

3.2.3. Residual Energy

Energy is consumed when a packet is received or sent or when a node is idle overhearing traffic from neighboring nodes. Energy consumption of a node can be determined using the following formula:

$$E_{\mathrm{c}}(n) = \left[P_{\mathrm{t}} \times \frac{D_{\mathrm{s}}}{D_{\mathrm{r}}} - P_{\mathrm{r}} \times \frac{D_{\mathrm{s}}}{D_{\mathrm{r}}} \right] + nP_{\mathrm{o}} \quad (3)$$

where $E_{\mathrm{c}}(n)$ is the energy consumed by the node, P_{t} is the power consumption for signal transmission, D_{s} is the size of the data packet, D_{r} is the transmission rate, P_{r} is the power consumption for the reception, and P_{o} is the power consumption during the period of overhearing the neighbor nodes.

Residual energy is available or remaining energy in a node which can be calculated as follows:

$$Er(n) = E_{\mathrm{i}}(n) - E_{\mathrm{c}}(n) \quad (4)$$

where $E_{\mathrm{i}}(n)$ is the amount of initial energy of a node and $E_{\mathrm{c}}(n)$ is the consumed energy of the node.

3.3. Trust Based Secure and QoS Routing Scheme

We describe the proposed trust-based secure QoS routing scheme (TSQRS) and its implementation in detail in this section. A trust model is employed in TSQRS to improve the cooperative routing and the performance of MANETs through evaluating the trustworthiness of the nodes in the networks. In the trust model, a node promiscuously listens to its neighboring nodes to evaluate the trust of these values. Due to the broadcast nature of MANETs, a node can observe and estimate the resources of a neighboring node through their direct interactions in a passive mode. When direct observation is involved, a complete history of trustworthiness can be provided by a node. Such a history would include information about communication quality of the node. In TSQRS, we include in our scheme the direct observations to derive trust values on neighboring nodes through using the social and the QoS trust parameters. In addition, trust is assessed on a continuous basis with a fixed time interval and trust value is calculated according to the quality of the behavior in packet forwarding by a node. The whole process continues until the destination node is found and an optimal and secure path from the source to the destination is formed. The selection of the intermediate nodes or the forwarding path is determined according to the trust feedback information. Following are the mechanisms that are used in our scheme for trust management:

- Trust recommendation using HELLO messages.
- Trust update.
- Trust based secure QoS routing strategy.

3.3.1. Trust Recommendation Using HELLO Messages

Figure 2 is the flowchart for the exchange of HELLO messages which are mostly used in the ad-hoc on demand distance vector routing protocol (AODV) to determine link connectivity. If each and every node keeps information about its neighboring nodes, it would help any node to make a better decision on routing. Since our routing scheme also uses HELLO messages to exchange QoS trust recommendations and to discover neighbors, we modify the HELLO packets to include some extra fields i.e., Residual Energy, Link Quality and Channel Quality as these parameters are the major reasons for unintentional node failure in mobile Ad hoc network affecting the QoS provided by MANET. Thus, QoS trust values are propagated through the HELLO packets. Each and every node periodically sends HELLO packets which incorporate the QoS parameters, allowing each node to obtain information about QoS trust values of its neighbors. Then, a node is trusted according to its QoS parameters values.

If a node that sends hello message is a trusted node, then, the intimacy with the sending node is calculated and the result is saved in a neighbor table to be used to build a suitable route for routing. Intimacy is an aggregation of direct interaction experience that determines the level of interaction with a sending node.

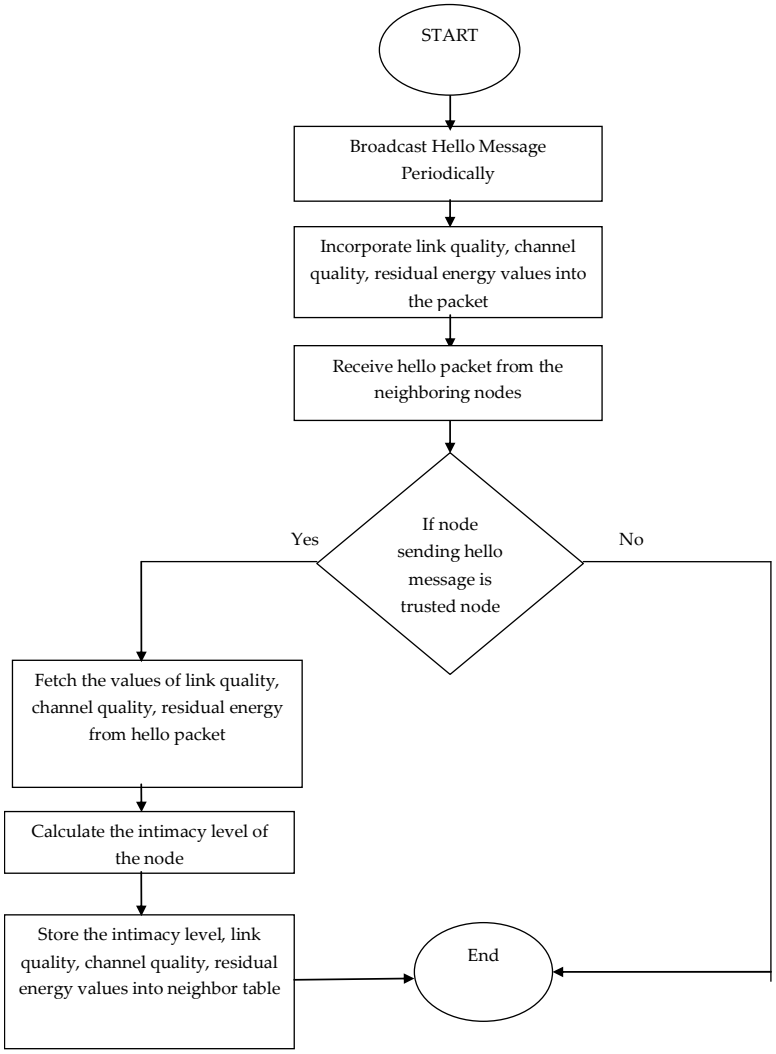

Figure 2. Trust recommendation using HELLO message exchange.

3.3.2. Trust Update

Our trust-based model takes the mobility of the network into account. Without further updates or continuous interactions between nodes, trust values would decay over time. Node mobility may also cause continuous interactions between a node and other group members, lowering the chance of nodes' evaluating each other in the same group. This includes cases such as breakage of links to a node, causing disconnection from the current group, voluntary disconnection (for saving power) or involuntary disconnection (due to physical terrain or low energy). We also assume the malicious behavior of individual nodes in resource-constrained MANETs. In a routing process, neighbor node's trust is evaluated by the sender by observing activities carried out by that neighbor and forwarding behaviors of neighbors. To be specific, a source node will observe the trust of its neighbor node based on its data forwarding behaviors and QoS parameters [5]. In our proposed trust-based model, we calculate historical trust consistently after a particular time interim called trust update so that we can identify all the nodes that behave maliciously and then update secure routes towards destinations by

updating information in the routing table. The overall neighbor trust value is derived based on the following equation:

$$Neighbor_{Trust} = w1 \times CFR + w2 \times DFR + w3 \times Intimacy_{level} + w4 \times Residual_{Energy} + w5 \times Link_{Quality} + w6 \times Channel_{Quality} \quad (5)$$

In Equation (5), *CFR* is the ratio of number of control packets forwarded correctly by a node against total number of control packets supposed to be forwarded, and DFR is the ratio of total number of data packets forwarded correctly by a node against total number of data packets supposed to be forwarded [23]. $w1$, $w2$, $w3$, $w4$, $w5$, $w6$ are the weights where $0 \leq w1, w2, w3, w4, w5, w6 \leq 1$ and $w1 + w2 + w3 + w4 + w5 + w6 = 1$. The values for the weights are purely decided by the empirical way. At the same time, they are decided by MANET application and QoS parameters that a user would give higher priority [24].

Meanwhile, according to the behavior of neighbor nodes, trust value varies over the time. We use trust threshold η for the nodes to differentiate malicious nodes from benign ones. During the whole trust update process shown in Figure 3, nodes having poor quality and false behavior are marked as malicious and the routing table is updated with the most recent routing information continuously in order to build optimal and secure paths.

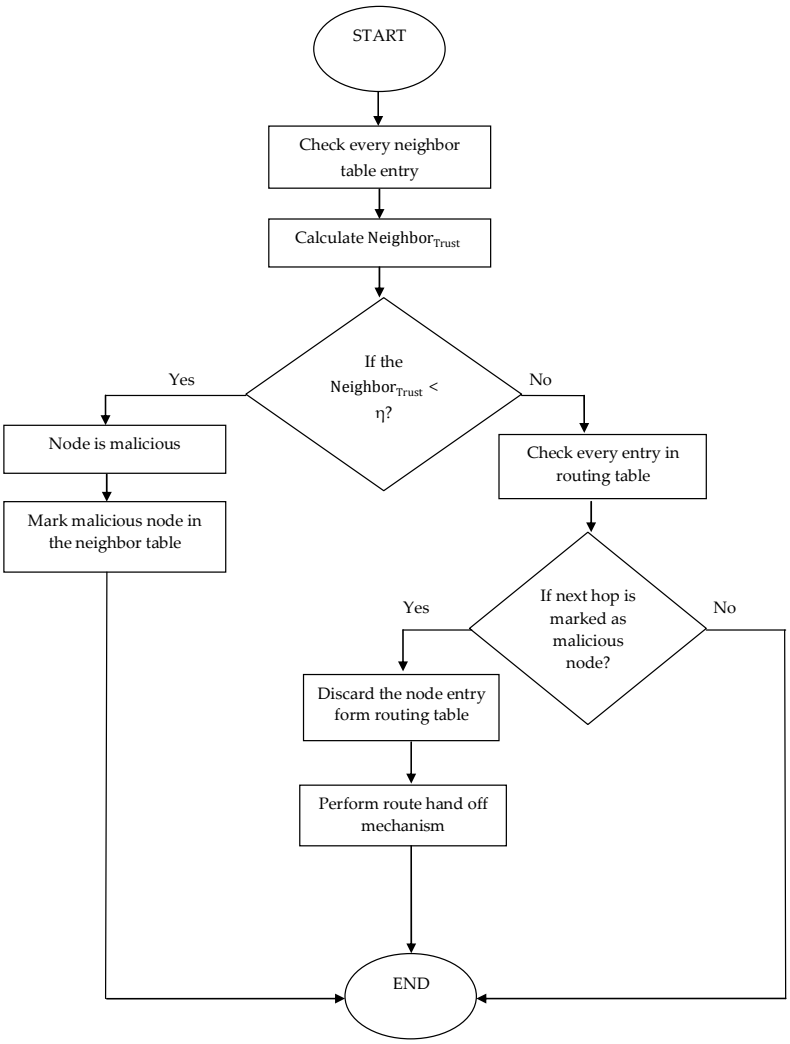

Figure 3. Trust update.

3.3.3. Trust Based Secure and QoS Routing Strategy

Figure 4 shows the flowchart for isolating a malicious node. All the nodes including the source, the intermediates, and the destination are cooperating during the route discovery process. The process of sending data towards the destination is as follows:

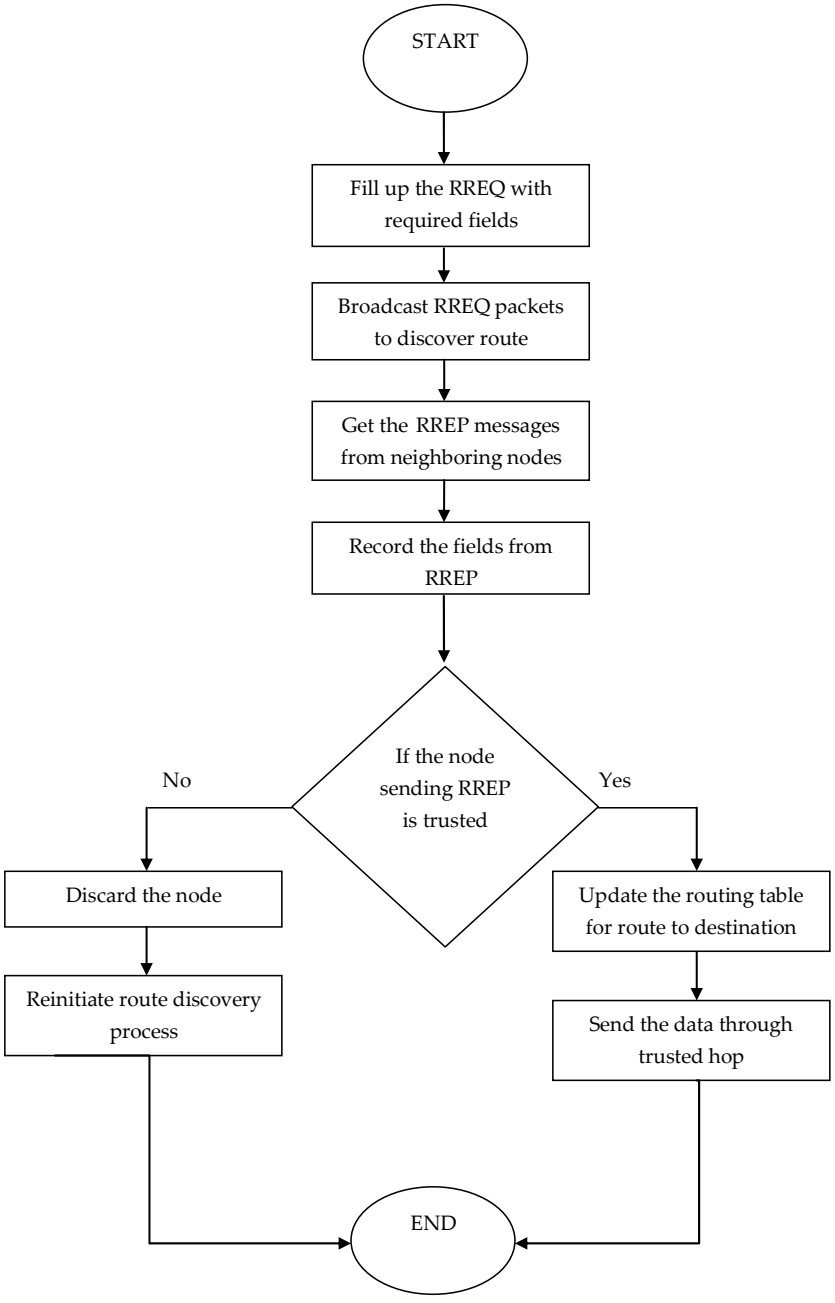

Figure 4. Trust based secure Qulaity of Service (QoS) routing strategy.

Before data transmission begins, the source node finds the entry of the destination node in its routing table. If such an entry exists, the data is sent to the destination through a trusted hop. Otherwise, the source node starts a route discovery process by flooding route request (RREQ) packets into the network to discover a route to the destination node.

During the routing process, if an intermediate node identifies a distrusted (marked as malicious during the trust update process) next hop in its routing table to the destination node, then the entry of

that particular node is discarded. The route discovery process is initiated by the intermediate node to discover an alternative trusted next hop.

After the destination node is found, the route reply (RREP) is sent back to the sender node through trusted hops. If more than one RREP are delivered to the source node than the route with the highest destination sequence number is chosen and a trusted route is created for the destination node and saved in the routing table for routing.

Finally, data is sent to the destination. If no routes are found, the whole process will repeat.

4. Simulation and Result Analysis

NS-2 (ver. 2.34) simulator system was utilized to evaluate the effectiveness of TSQRS with the adversary model. We performed the simulation for two scenarios: (1) by varying the mobility of nodes and (2) by varying the number of malicious nodes. We use packet drop ratio (PDR), routing overhead (RO), energy consumption (EC) to assess the performance of our proposed scheme. To show that TSQRS can achieve better routing decisions, the performance of TSQRS is compared to ETRS-PD and AODV with the adversary model. We carried out our simulations in a 1000×1000 m^2 area and employed IEEE 802.11 MAC. The benign nodes were distributed randomly throughout the network which employs the AODV, ETRS-PD and TSQRS protocols. Randomly positioned nodes perform various packet forwarding misbehaviors according to the adversary model. Table 1 summarizes the simulation parameters.

Table 1. Simulation parameters. Constant Bit Rate (CBR); User Datagram Protocol (UDP).

Parameter	Value
Simulator	NS 2.34
Routing Protocol	AODV, Adversary Model, TSQRS
Scenario Size	1000×1000 m^2
Number of Nodes	50
Misbehaving Nodes	0–40%
Simulation Time	240 s
Traffic Type	CBR/UDP
Number of connections	15
Pause Time	5 s
Mobility	4–20 m/s

4.1. Evaluation Considering Node Mobility

In this experiment, the performance of the protocols is assessed by changing the mobility of the nodes between 4–20 m/s while other parameters stay constant. The percentage of malicious nodes is fixed to 20%.

Packet delivery ratio (PDR): As shown in Figure 5, as the mobility increases from 4 to 20 m/s, PDR of AODV decreases from around 50 to 37% while that of ETRS-PD decreases from around 71 to 52%. As the speed gets higher, there is an expanded number of link failures, causing packet loss. TSQRS shows improvement in PDR from 85 to 75% compared to AODV and ETRS-PD. As mobility level increases, there are an increasing number of link breakages, resulting in more path failure and unusual packet loss.Ways of improving the result include (1) using the secure route to the destination and (2) considering link quality for the selection of forwarding node.

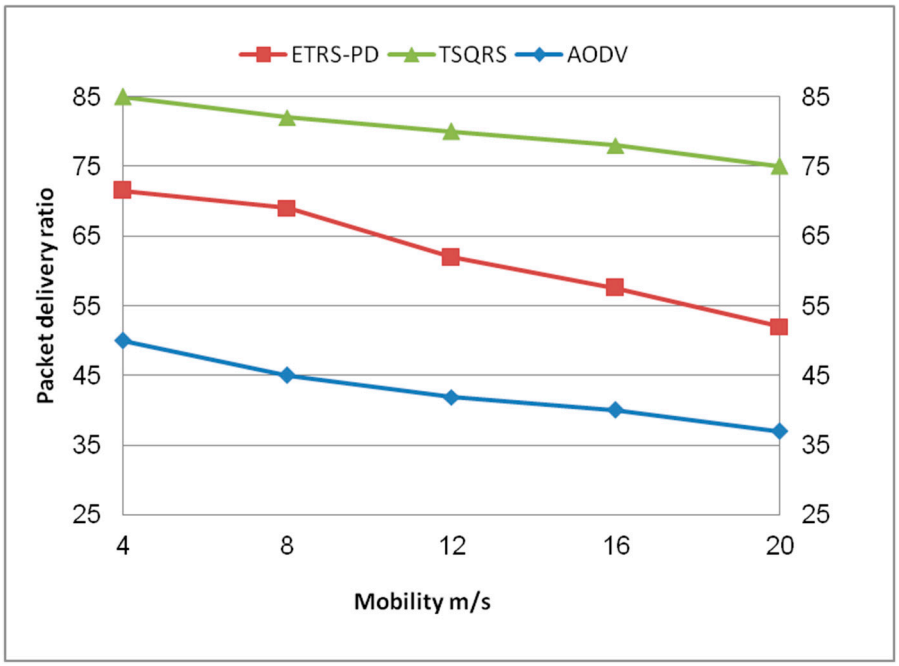

Figure 5. Packet delivery ratio (PDR) against mobility.

Routing overhead (RO): As shown in Figure 6, RO of AODV is between 4.5 and 8.5 while that of ETRS-PD is between 2.7 and 7.07 which is somewhat improved. Meanwhile, the RO of TSQRS shows great improvement with values between 1.64 and 4.8. High mobility leads to more frequent path failure and route discovery, resulting in higher routing overhead. In TSQRS, the selection of intermediate nodes is based on QoS parameters which would lower the routing overhead.

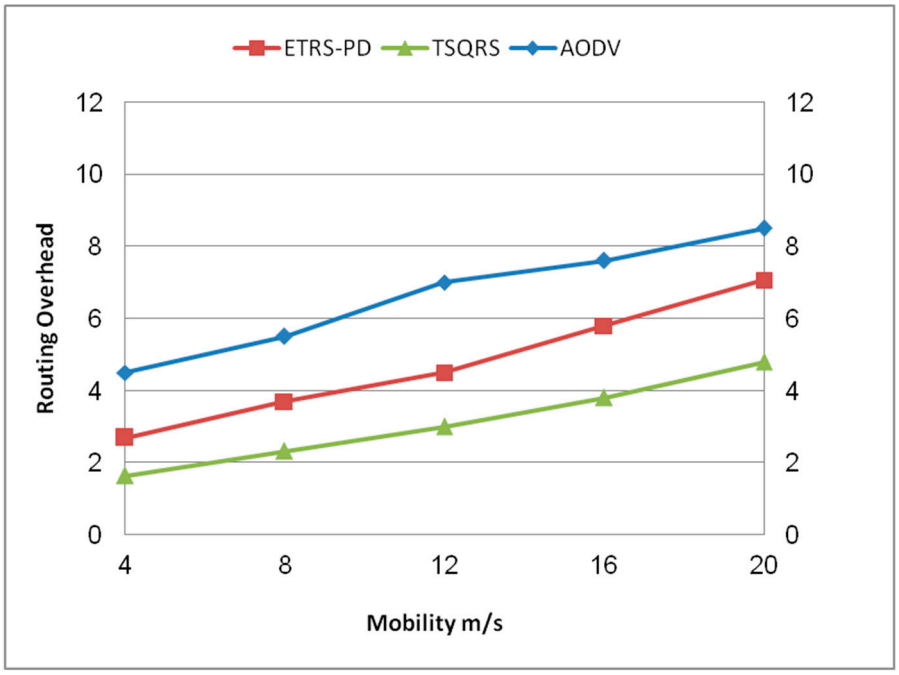

Figure 6. Routing overhead (RO) against mobility.

Energy consumption (EC): We also analyzed the performance of ETRS-PD and TSQRS in terms of energy consumption. As shown in Figure 7, EC of ETRS-PD is between 313.96 and 314.53 J under the adversary model while TSQRS provides improved results, i.e., between 310.2 and 310.9 J. EC depends upon the number of packets sent and received. More link failures reported by a protocol would result in a large amount of energy consumption in the network. TSQRS consumes less energy because it considers link quality and residual energy in the nodes for routing.

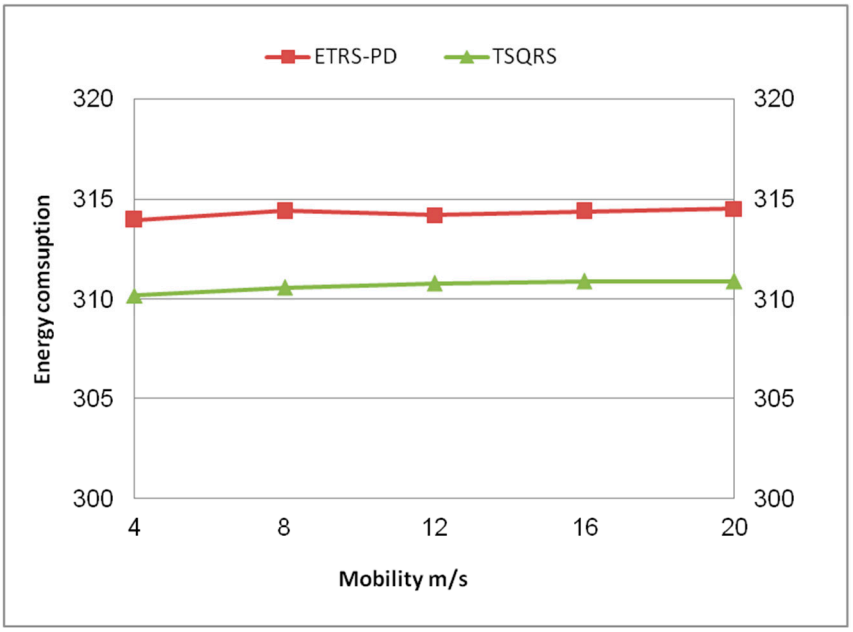

Figure 7. Energy consumption (EC) against mobility.

4.2. Evaluation Considering thePercentage of Malicious Nodes

In this experiment, the three protocols were evaluated against the same adversary model and by varying the percentage of malicious nodes between 0 and 40% with other parameters being kept fixed. Especially, the mobility parameter is constant at 20 m/s.

Packet delivery ratio (PDR): As shown in Figure 8, as the percentage of malicious nodes increases, there is an expansion in the number of packet drops in which PDR of AODV decays to about 30% under the adversary model while ETRS-PD provides some improvement to nearly 51.67%. TSQRS shows an improvement in PDR compared to AODV and ETRS-PD to achieve 60%. Trust mechanism that is used in TSQRS to judge the false behavior of neighboring nodes helps to eliminate the malicious nodes during routing, which in turn reduces the number of dropped packets.

Routing overhead (RO): The RO of AODV fluctuates in the range 4.8 to 9.9 under the adversary model as shown in Figure 9. ETRS-PD again enhances RO to the range of 4.8 to 6.5 when contrasted to AODV. TSQRS achieves further improvement in RO. It is clear that the more the number of malicious nodes, the more easily they can cause damage. Since TSQRS selects only those nodes that are secure and have good link quality, there is a lower number of route failures, causing less number of control packets to be re-forwarded for route establishment.

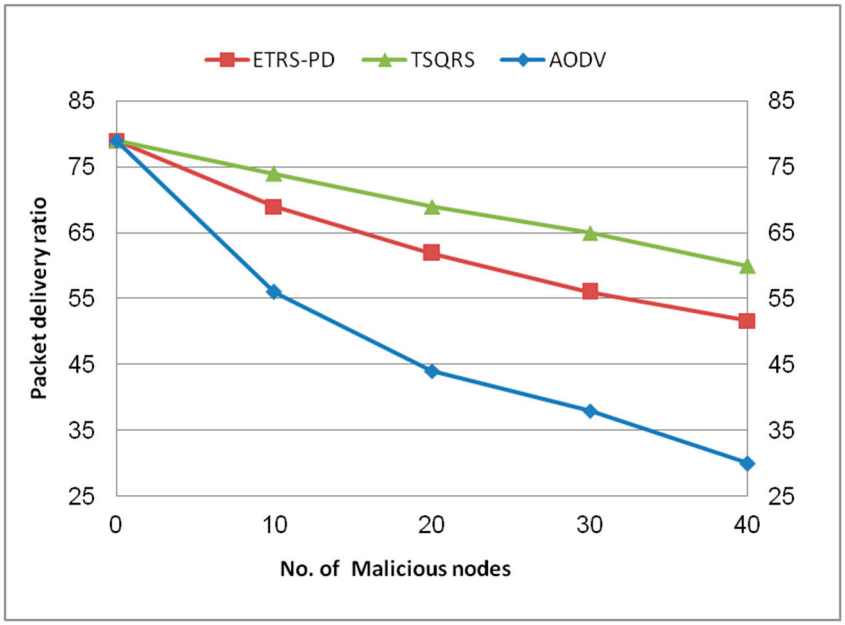

Figure 8. PDR against percentage of malicious nodes.

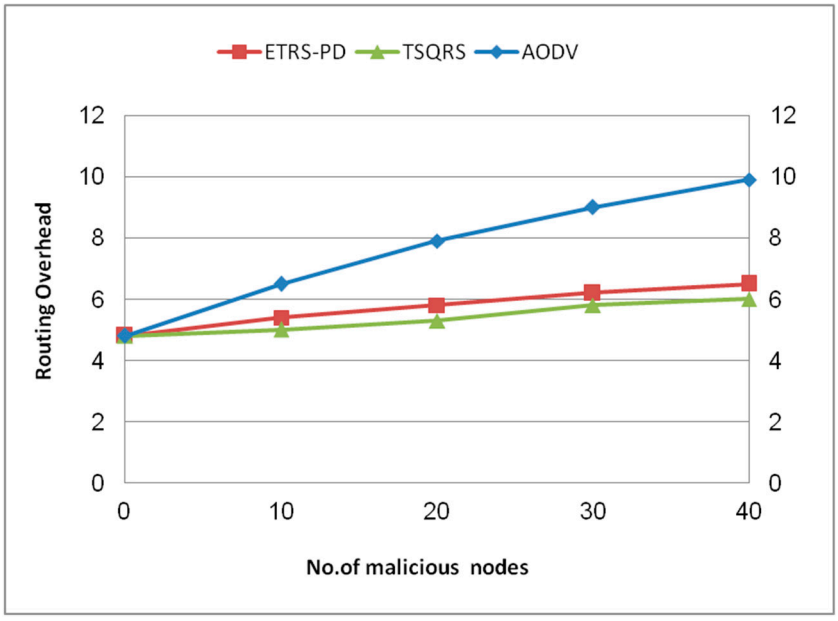

Figure 9. RO against percentage of malicious nodes.

Energy consumption (EC): As shown in Figure 10, under the adversary model, EC in ETRS-PD varies between 311.96 to 313.5 J while TSQRS provides an improvement to achieve 310.36 to 309 J, a difference of 1.6 and 4.5 J, respectively. Thus, TSQRS is more energy efficient compared to ETRS-PD in different percentages of malicious nodes due to fewer route failures.

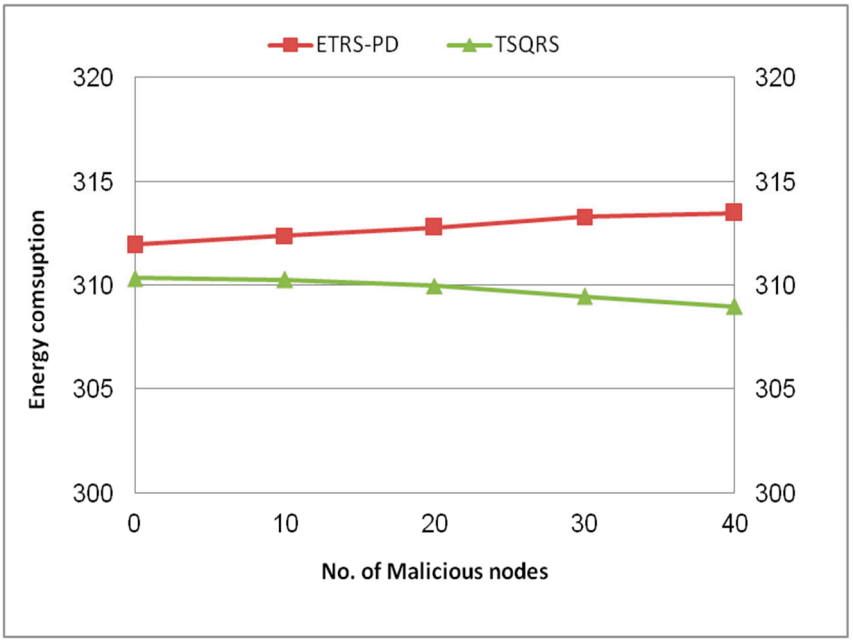

Figure 10. EC against percentage of malicious nodes.

5. Conclusions

As a part of the literature survey, we observed that integration of QoS trust and social trust could improve the performance of routing in MANETs as both quality and security are very important aspects of such networks. Considering these notes, we developed a trust-based scheme, called TSQRS, in which both components are incorporated. To facilitate reliable communication in the highly dynamic environment of MANETs, TSQRS considers three important parameters during the discovery of on-demand routes, i.e., channel quality, link residual life and residual energy, to reduce route failures and to increase the overall system performance. In addition, the use of CFR, DFR and intimacy level during trust update plays an important role in removing malicious nodes during the routing process. Performance comparison of TSQRS to ETRS-PD and AODV under the same adversary model shows that TSQRS can improve consistently packet delivery ratio, routing overhead and energy consumption due to the enhancement to the routing process and due to the inclusion of new trust components for improving and securing the routing process. Many future works are possible in this area. It is possible to use intelligent rules to make effective decisions in routing. Adaptation of intelligent prediction functions such as software agents for evaluating nodes capability and reliability are suitable where the environment is unreliable, unpredictable and much dynamic. Intelligent Agents can be deployed at each sensor node to accurately predict the resource availability and reliability in order to perform organized allocation of the resource before the data routing.

Acknowledgments: The work in this paper has been supported by National Natural Science Foundation of China (No. 61602456) and National High Technology Research and Development Program of China (863 Program) (No. 2015AA017204).

Author Contributions: Nafei Zhu and Jingsha He, Ideas, general approach and overall supervision; Muhammad Salman Pathan, model design, experiment and analysis; Zulfiqar Ali Zardari and Muhammad Qasim Memon, contributed reagents/materials/analysis tools; Muhammad Iftikhar Hussain, discussion and paper editing.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sumathi, K.; Priyadharshini, A. Energy Optimization in MANETs Using On-demand Routing Protocol. *Procedia Comput. Sci.* **2015**, *47*, 460–470. [CrossRef]
2. Kuo, W.K.; Chu, S.H. Energy Efficiency Optimization for Mobile Ad Hoc Networks. *IEEE Access* **2016**, *4*, 928–940. [CrossRef]
3. Hinge, R.; Dubey, J. Opinion based trusted AODV routing protocol for MANET. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), Udaipur, India, 4–5 March 2016; ACM: New York, NY, USA, 2016.
4. Venkanna, U.; Agarwal, J.K.; Velusamy, R.L. Cooperative Routing for MANET Based on Distributed Trust and Energy Management. *Wirel. Pers. Commun.* **2015**, *81*, 961–979. [CrossRef]
5. Malathi, M.; Jayashri, S. Robust against route failure using power proficient reliable routing in MANET. *AEJ J.* **2016**. [CrossRef]
6. Chavhan, S.; Venkataram, P. Emergent Intelligence Based QoS Routing in MANET. *Procedia Comput. Sci.* **2015**, *52*, 659–664. [CrossRef]
7. Gite, P.; Kanellopoulos, D.; Choukse, D. An extended AODV routing protocol for secure MANETs based on node trust values. *Int. J. Int. Tech. Secur. Trans.* in press.
8. Koul, A.; Kaur, H. Quality of Service Oriented Secure Routing Model for Mobile Ad hoc Networks. In Proceedings of the International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence, Hong Kong, China, 25–27 March 2017.
9. Zafar, S.; Soni, M.K. Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET. In Proceedings of the International Conference on Reliability Optimization and Information Technology, Faridabad, India, 6–8 February 2014.
10. Shah, S.N.; Jhaveri, R.H. A trust-based scheme against Packet dropping attacks in MANETs. In Proceedings of the 2nd International Conference on Applied and Theoretical Computing and Communication Technology, Banglore, India, 21–23 July 2016.
11. Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. In *Ad Hoc Netw.*; Ortiz, J.H., de la Cruz, A.P., Eds.; InTech: London, UK, 2017; ISBN 978-953-51-3109-0.
12. Singal, G.; Laxmi, V.; Gaur, M.S.; Todi, S.; Rao, V.; Tripathi, M.; Kushwaha, R. Multi-constraints link stable multicast routing protocol in MANETs. *Ad Hoc Netw.* **2017**, *63*, 115–128. [CrossRef]
13. Jhaveri, R.H.; Patel, N.M. Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. *IJCS* **2017**, *30*. [CrossRef]
14. Sarkar, S.; Datta, R. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. *Ad Hoc Netw.* **2016**, *37*, 209–227. [CrossRef]
15. Sirisala, N.; Bindu, C.S. A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets. *Int. J. Intell. Eng. Syst.* **2016**, *10*, 116–125. [CrossRef]
16. Khamayseh, Y.M.; Aljawarneh, S.A.; Asaad, A.E. Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. *Sustain. Comput. Inform. Syst.* **2017**, in press. [CrossRef]
17. Sethuraman, P.; Kannan, N. Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. *Wirel. Netw.* **2017**, *23*, 2227–2237. [CrossRef]
18. Ahmed, M.N.; Abdullah, A.H.; Chizari, H.; Kaiwartya, O. Flooding Factor based Trust Management Framework for secure data transmission in MANETs. *J. King Saud Univ. Comput. Inf. Sci.* **2017**, *29*, 269–280. [CrossRef]
19. Kambourakis, G.; Konstantinou, E.; Douma, A.; Anagnostopoulos, M.; Fotiadis, G. Efficient Certification Path Discovery for MANET. *EURASIP J. Wirel. Commun. Netw.* **2010**, *2010*, 243985. [CrossRef]
20. Rajkumar, B.; Narsimha, G. Trust Based Certificate Revocation for Secure Routing in MANET. *Procedia Comput. Sci.* **2016**, *92*, 431–441. [CrossRef]
21. Cho, J.-H.; Chen, I.-R.; Kevin, S.J. Trust threshold based public key management in mobile ad hoc networks. *Ad Hoc Netw.* **2016**, *44*, 58–75. [CrossRef]

22. Jhaveri, R.H.; Patel, N.M. A Sequence Number Based Bait Detection Scheme to Thwart Grayhole Attack in Mobile Ad Hoc Networks. *Wirel. Netw.* **2015**, *21*, 2781–2798. [CrossRef]
23. Xia, H.; Jia, Z.; Li, X.; Ju, L.; Sha, E.H.-M. Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Netw.* **2013**, *11*, 2096–2114. [CrossRef]
24. Mylsamy, R.; Sankaranarayanan, S. A Preference-Based Protocol for Trust and Head Selection for Cluster-Based MANET. *Wirel. Pers. Commun.* **2016**, *86*, 1611–1627. [CrossRef]