ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Trust Based Routing Protocol for Multi-Hop Wireless Networks

A.K.Chakravarthy[1]
M.Tech.Scholar
Department of Computer Science & Engineering
Sri Sai Aditya Institute of Science and Technology,
Surampalem,
Kakinada, Andhra Pradesh – India

B. Durga Anuja[2]
Assistant Professor
Department of Computer Science & Engineering
Sri Sai Aditya Institute of Science and Technology,
Surampalem,
Kakinada, Andhra Pradesh – India

AbstractIn a multi-hop wireless Network the mobile nodes acts as a router to forward packets, which are generated from the other nodes. There is no fixed infrastructure for routing purpose. The multi-hop wireless Network nodes need to spare their resources and time in order to accomplish this task. However malicious nodes do not co-operate but makes use of fairness and performance of the network. These type of nodes reduces the network performance. In this paper, we propose a Trust based routing protocol for multi-hop wireless Networks TBRP (Trust Based Routing Protocol) based on Trust value. In this The Trust Value (TV) plays a vital role in the route detection. The TV can be calculated based on the low mobility, broken links and large hardware resources. Based on the Trust value we will route message through highly trusted nodes to minimize the probability of dropping the message and thus improve the network performance.

Keywords: Network, Multi-hop, Message, malicious node, Trust based, trusted value, RREP, RDP, DACK.

I. INTRODUCTION

The interest in multi-hop wireless networks (such as Mobile Ad-hoc NETworks (MANETs), Vehicular Ad-hoc NETworks (VANET), Multi-hop Cellular Networks (MCNs) or Wireless Mesh Network (WMN)) has been increasing significantly [1- 4]. Multi-hop relaying has been gaining global acceptance as one of the most promising technologies in next-generation wireless networks. Recently, many research works have been appeared to extend the traditional one-hop wireless network access to multi-hops networks [5,6], i.e., traffic originated from a mobile node is relayed through the network nodes to the destination. Multi-hop relaying enables many types of applications and enhances the network performance and deployment. In infrastructure rich areas, it can extend communication range using limited transmit power, improve area spectral efficiency, reduce the dead areas, and enhance the throughput and network capacity [7, 8]. Vehicular ad hoc network is a recent civilian application to deploy multi-hop relaying [9]. In civilian applications, malicious nodes will not be voluntarily interested in cooperation without sufficient incentive however; they use the honest nodes to relay their packets without any contribution to the network, which has negative effect on fairness, performance and security. Fairness issue arises when a malicious node practically takes advantage from the cooperative nodes by using the network without contributing to it. The malicious nodes significantly degrade the network performance resulting in failure of multi-hop data communication [10].

There are two primary motivations associated with trust management in MANETs. At first, trust evaluation helps distinguish between good and malicious entities. Creating trust history, one entity can remember others' behaviors. This memory provides a method for good entities to avoid working with suspect ones. Secondly, trust management offers a prediction of one's future behavior and improves network performance.

In this paper we propose a Trust Based Routing Protocol (TBRP) to increase network performance. In a route discovery, this protocol is able to create multiple loop-free paths between a source and a destination through hop-by-hop route. Each route has a cost vector composed of hop count and trust value. Furthermore, this protocol provides a flexible and feasible approach to choose a shortest path.

II. RELATED WORK

In The multi-hop wireless network Routing is an essential functionality. In order to achieve this functionality in a optimistic way different routing protocols have been put by various authors .Existing Routing Protocols focuses on different issues: Routing misbehavior in multi- hop wireless network, Trust value management and Node selection and Routing.

A. Compromised routing in multi-hop wireless network

In multi-hop wireless networks (MWNs), the traffic originated from a node is usually relayed through the other nodes to the destination for enabling new applications and enhancing the network performance and deployment [11]. But in the multi-hop wireless network malicious nodes do not relay other nodes' packets and makes use of the cooperative nodes to relay their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the malicious nodes' cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment [12].

The technique involved in the secure cooperation incentive protocol that uses the public-key operations only for the first packet in a series and uses the light-weight hashing operations in the next packets, so that the overhead of the packet series converges to that of the hashing operations. Hash chains and keyed hash values are used to achieve payment non repudiation and prevent free riding attacks.

B. Trust value management in multi-hop wireless network

The trust values are calculated from each node based on nodes' trustworthiness and reliability in relaying packets. It is fair to increase the trust values of the nodes that are not in broken links, because they relayed packets truthfully. On the other hand, the trust system decreases the trust values of the two nodes in a broken link. Trust is also dynamic or time-sensitive. So trust party has to periodically evaluate the nodes' trustworthiness, i.e., a trust value at time t may be different from its value at another time. So the proposed system relies on the multi-dimensional trust values instead of single trust value to precisely predict the nodes' future behavior. Trust values are used to decide which nodes to select or avoid in routing. Since a trust value depicts the probability that the node conducts an action, route reliability can be computed using its nodes' trust values to give probabilistic information about the route stability and lifetime.

C. Node selection and Routing.

Traditional routing protocols in ad hoc network can be categorized into two primary types: proactive and reactive [6]. Proactive routing protocols establish and maintain routes at all instants of time in order to avoid the latency during new route discoveries. Reactive routin protocols do discovery route only when one node tries to transmit packets to another unknown route node so as to save resources. The nodes in an ad hoc network generally have limited resources, such as bandwidth and power energy; therefore.

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm the main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used.

III. TBRP NETWORK ARCHITECTURE

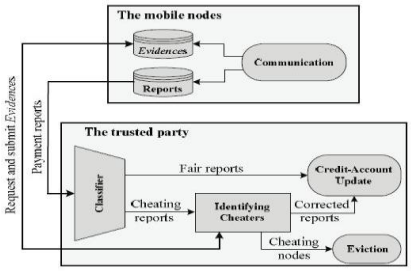

Fig 1.TBRP Network architecture

The multi-hop wireless networks have mobile nodes and Trusted Party (TP) whose public key is known to all the nodes. The mobile nodes have different hardware and energy capabilities. The network is used for civilian applications, its lifetime is long, and the nodes have long relation with the network. Thus, with every interaction, there is always an expectation of future reaction. Each node has a unique identity and public/private key pair with a limited-time certificate issued by TP. Without a valid certificate, the node cannot communicate nor act as an intermediate node. TP maintains the nodes' credit accounts and trust values. Each node contacts TP to submit the payment reports and TP updates the involved nodes' payment accounts and trust values.

IV. PROPOSED METHOD

Problem Definition

In the multi-hop wireless network malicious nodes do not relay other node's packets and makes use of the cooperative nodes to relay on their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the malicious nodes' cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment.

B. Proposed Trust-based Scheme

As nodes in MWN networks have a limited transmission range, they expect their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat the nodes available in the network. This assumption becomes invalid when the nodes in the network have tangential or contradictory goals. The Trusted party calculate trust value for each node based on their value of the nodes, based on their past history of relaying packets, and link failures, can be used by their neighbors to ensure that the packet will be relayed by the node.

C. Design Requirements

The following requirements are set while designing the Trust-based routing protocol:

- The Trust value information should be easy to use and the nodes should be able to ascertain the best available nodes for routing without requiring human intervention.
- Nodes should be able to communicate to the trusted party to get the network information.
- The collection and storage of nodes' trust values are done in a centralized way.
- The Trust value information is dynamically broadcasted by the trusted party to the nodes in the network.

In the proposed trust based scheme, all the nodes in the mobile ad hoc network will be assigned an initial value of null (0) as in the ocean reputation-based scheme. Initially Node sends RREP to the first received RDP packet of a specific sender only, the destination will uncast a RREP for each RDP packet it receives and forward this RREP on the reverse-path. The next-hop

node will relay this RREP. This process continues until the RREP reaches the sender. After that, the source node sends the data packet to the node with the highest trust value. Then the intermediate node forwards the data packet to the next hop with the highest trusted node and the process is repeated till the packet reaches its destination. The destination acknowledges the data packet (DACK) to the source that updates its reputation table by giving a recommendation of (+1) to the first hop of the reverse path.

All the intermediate nodes in the route give a recommendation of (+1) to their respective next hop in the route and update their local trust tables. If there is a malicious node in the route, the data packet does not reach its destination. As a result, the source does not receive any DACK for the data packet in appropriate time. So, the source gives a recommendation of (-1) to the first hop on the route. The intermediate nodes also give a recommendation (-1) to their next hop in the route up to the node that dropped the packet.

As a consequence, all the nodes between the malicious node and the sender, including the malicious node, get a recommendation of (-1). The idea of giving (-1) to malicious nodes per each data packet dropping is due to the fact that negative behavior should be given greater weight than positive behavior. In addition, this way prevents a malicious node from dropping alternate packets in order to keep its reputation constant. This makes it more difficult for a malicious node to build up a good trust value to attack for a sustained period of time. Moreover, the malicious node will be isolated if its reputation reached a threshold of (-50) as in the Ocean reputation-based scheme. In the following table, the default Trust Based parameters are listed in the below table.

Table 1: Trust based parameters

Initial Trust value	0
Trusted node min value	+1
Malicious node value	-1
Trust Threshold value	-50

There are mainly three phases in the algorithm as mentioned below

Step 1: Trust computation Phase

Step 2: Route establishment Phase

Step 3: Data Transfer Phase

Step 4: Trust computation Phase

Trust Party receives a report, it first checks if the report has been processed before using its unique identifier. Then, it verifies the authority of the report by computing the node signatures with hash message. If the report is valid, trust party verifies the destination node's hash message. TP clears the report by rewarding the intermediate nodes and debiting the source and destination nodes. The number of sent message is signed by the source node and the number of delivered messages can be computed from the number of hashing operations done.

The trust values are calculated from each node based on nodes' trustworthiness and reliability in relaying packets. It is fair to increase the trust values of the nodes that are not in broken links, because they relayed packets truthfully. On the other hand, the trust system decreases the trust values of the two nodes in a broken link. Trust is also dynamic or time-sensitive. So trust party has to periodically evaluate the nodes' trustworthiness, i.e., a trust value at time t may be different from its value at another time. So the proposed system relies on the multi-dimensional trust values instead of single trust value to precisely predict the nodes' future behavior. Trust values.

Step 2: Route establishment Phase

In this route establishment phase we will use destination sequenced distance vector (DSDV) routing algorithm to perform routing. This protocol avoids the low-trusted nodes..The RREQ packet contains the identities of the source and destination nodes, the maximum number of intermediate nodes, trust and energy requirements and the source node's signature and certificate then the source node is trust requirements are verified at each intermediate node can have low trust values, then verified at each subsequent intermediate nodes till it reaches at the highly trusted nodes. Each intermediate node ensures that it can satisfy the source node's trust/energy requirements. It also verifies the packet's signature using the public keys extracted from the nodes' certificates. These verifications are necessary to ensure that the packet is sent and relayed by genuine nodes and the nodes can satisfy the trust requirements.

Step 3: Data Transfer Phase

At this time, the source node S and the other intermediate nodes have many RREPs for the same RDP packet sent earlier. So, the source node S chooses the highly-reputed next-hop node for its data transfer. If two next-hop nodes have the same reputation, S will choose one of them randomly, stores its information in the sent-table as the path for its data transfer. Also, the source node will start a timer before it should receive a data acknowledgement (DACK) from the destination for this data packet. Afterwards, the chosen next-hop node will again choose the highly-reputed next-hop node from its routing table and will store its information in its sent-table as the path of this data transfer. Also, this chosen node will start a timer, before which it should receive the DACK from the destination for this data packet. This process continues till the data packet reaches the destination node D.

V. CONCLUSION

In this paper we have described Trust Based Routing Protocol (TBRP) based on the trust value. Combined with the model, a destination sequence distance vector routing algorithm is used to perform routing. This protocol provides a flexible and feasible approach to choose a shortest path in all trusted paths to meet the dependable or trust requirements of data packets. For future work, we plan to extend our trust model to other ad hoc network routing protocols, and to compare performance of TBRP with other trust-based routing protocols.

References

1. S. Yang, and H. Chou, "Design Issues and Performance Analysis of Location- Aided Hierarchical Cluster Routing on The MANET", Proc. of IEEE CMC'09, Vol. 2, pp. 26-31, Kunming, Yunnan, China, January 6-8, 2009.
2. A. Amoroso, M. Roccetti, M. Nanni, and L. Prati, "VANETS without Limitations: An Optimal Distributed Algorithm for Multi-hop Communications", Proc. of IEEE CCNC' 09, pp.1-5, Las Vegas, Nevada, USA, January 10-13, 2009.
3. X. Li, B. Seet, and P. Chong, "Multihop Cellular Networks: Technology and Economics", Computer Networks, Vol. 52, No. 9, pp. 1825 1837, June 2008.
4. O. Bazan, and M. Jaseemuddin,"Routing and Admission Control for Wireless Mesh Networks With Directional Antennas", Proc. of IEEE WCNC09, pp. 1-6, April 5-8, 2009.
5. G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin,"Multi-Hop Relay for Next- Generation Wireless Access Networks", Bell Labs Technical Journal, Vol. 13, No. 4, pp. 175-193, 2009.
6. F. Hossain, and H. Chowdhury, "Impact of Mobile Relays on Throughput and Delays in Multihop Cellular Network", Proc. of IEEE ICWMC' 08, pp. 304-308, Athens, Greece, July 27-August 1, 2008.
7. S. Narayanaswamy, V. Kawadia, R. Sreenivas, and P. Kumar, "Power Control in Ad Hoc Networks: Theory, Architecture, Algorithm and Implementation of The COMPOW Protocol", Proc. of European Wireless Conference, pp. 156-162, Florence, Italy, February 25–28, 2002.
8. P. Gupta, and P. Kumar, "The Capacity of Wireless Networks", IEEE Transactions on Information Theory, Vol. 46, No. 2, pp. 388-404, March 2000.
9. Y. Khaled, M. Tsukada, J. Santay, and T. Ernst, "On the Design of Efficient Vehicular Applications", Proc. of IEEE VTC' 09, Barcelona, Spain, April 26–29, 2009.
10. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. of IEEE/ACM MobiCom' 00, pp. 255–265.
11. G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009
12. Shilpa S G , Mrs. N.R. Sunitha, B.B. Amberker, "A Trust Model for Secure and QoS Routing in MANET", International Journal of Innovative Technology & Creative Engineering (ISSN: 2045-8711), vol.1no.5 may 2011.

