TRUST BASED ROUTING PROTOCOL FOR AD-HOC AND SENSOR NETWORKS

ABHISHEK GOWDA TV[1], DARSHAN GOWDA V[2], PARINITH KV[3], RAKESH P[4], Dr. SHABANA SULTANA[5]

[1234]Department of Computer Science and Engineering, The National Institute of Engineering(NIE) Mananthavady Road, Mysuru – 570008, Karnataka, India
[5]Department of Computer Science and Engineering ,Mysuru

Abstract - *Routing protocols in mobile ad hoc and sensor networks discover usable multi-hop routes between source and destination nodes. However, some of the routes found and used may not be as reliable or trustable as expected. Thus, finding a trusted route is an important component for enhancing the security of communication. This paper presents a trust-based routing protocol for enhanced security of communication in mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). Enhanced trust and security are achieved by the maintenance of a trust factor by the nodes in the network. This factor is established and refined over time and it increases for each node when it participates successfully in data transmissions. Simulation experiments are performed to verify the operation of the proposed protocol and evaluate its performance. The results show an improvement in the trust potential of the discovered path with the proper choice of certain important trust parameters.*

Key Words: **Wireless network, Trust, Quality of Service (QoS), Mobile ad hoc network (MANET), Wireless Sensor Network (WSN), Routing Protocol**

1. INTRODUCTION

In a mobile ad hoc network (MANET), nodes cooperate to dynamically establish the network configuration and find and maintain routes for message exchange. A similar strategy is used in wireless sensor networks (WSNs) which are considered a derivative of MANETs with some differences. Such differences include a larger number of nodes and less node mobility in WSNs. In both networks, nodes are responsible for forwarding packets for each other to facilitate multi-hop communication between other nodes that are not in direct transmission range. However, the lack of a fixed topology in these networks leads to significant challenges to the routing process. Particularly, when the issue of trust among the nodes is in question. Routing protocols designed for ad hoc networks such as the Dynamic Source Routing protocol (DSR) , and the Ad hoc On-Demand Distance Vector (AODV) protocol are generally effective and efficient. However, different nodes exhibit different measures of trust and reliability to effectively and correctly participate in the routing and data transmission process. Routing protocols were investigated and modified, and new protocols were introduced to enhance the routing process in such networks. Many of these protocols provide some solution to parts of the problem.

Our approach provides a routing protocol based on trust, which is established and maintained by the nodes in the network. In each node, the trust factor is updated based on the successful participation of the other nodes in previous data transmissions. Our protocol is based on the DSR routing protocol and is on-demand. In addition, it is a distributed protocol. Unlike other protocols, such as the link-state-based ones, each node only has to maintain topology and trust information about its immediate neighbors and not the entire network. These characteristics enhance the scalability and performance of our proposed algorithm.

2. RELATED RESEARCH

A lot of work has been done to offer better and secure routing protocols for ad hoc and sensor networks. Several factors are involved in this routing process. The unique characteristics of these networks have significant effects on the ability of the protocol to perform well. The issues of trust and security are very important for many communication environments and thus it is important to find efficient protocols that can address them. The authors in discuss a trust model for ad hoc networks and discuss how trust levels can be obtained and used. This model can discover a potentially trustable route for communication and data transmission. Initially, each node in the system is authenticated by an authentication mechanism and is assigned a trust value according to its identity.

3. THE PROPOSED SYSTEM

In this protocol we will keep track of the success rate (no of packets delivered successfully) for each route. Hence each node has a trust factor to trust its neighbors. Thus, avoiding the retransmission of the lost data and enhancing the existing protocol.

Route discovery messages are multicasted instead broadcasting to their neighbors which satisfies the eligibility criteria, thus avoiding the network traffic.

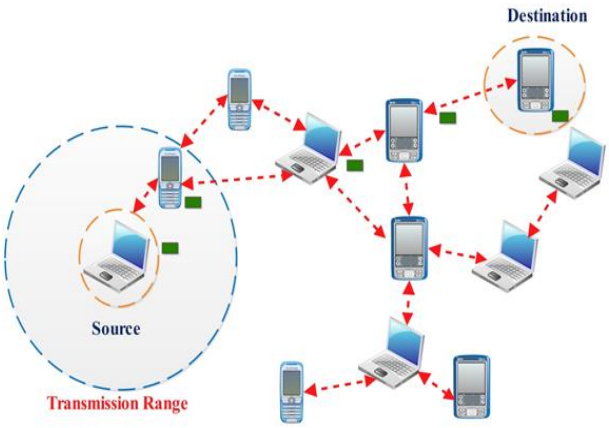

Fig-1: Proposed System Architecture

4 IMPLEMENTAION MODULES

4.1 1 Hop Neighbor Identification Module

1. Each node identifies its 1 hop neighbors using HELLO Exchange (UDP)

2. Each node broadcasts HELLO message to all 1 hop neighbors

3. Each identified 1 hop neighbors are set with MAX_TRUST=10

4.2 Route Request Transmission Module

1. Based on TRAS (Modified DSR) (Trust Routing Protocol) (UDP for RREQ & RREP)

2. RREQ (Route Request) Message Parameters:
   s-SourceIP, d-DestinationIP, ID-MessageID (To Avoid Looping)
   x-CurrentNodeIp Forwarding the RREQ
   tmin-Minimum trust value required, tcum Cumulative trust factor of the path
   PATH-Accumulated list of hosts that the RREQ message passed through
   MAX_NH-Maximum number of nodes in NH list (To control the flooding and provide better QOS)
   BACKUP_PATHS-Maximum number of backup paths required by Source Node (Default 0)

4.3Intermediate Node Decision Module

1. Uses Intermediate Node Algorithm

2. When an intermediate node receives RREQ, it sorts all of its 1-hop neighbors in descending order using their node trust factors

3. Current Node then adds its own trust factor to the tcum and further multicast to select its 1-hop neighbor

4.4 Route Reply Transmission Module

1. Destination might receive many RREQs

2. Destination node calculates Path Trust Factor (PTF) for every RREQ path i.e. PTF=tcum/n, where n is the number of intermediate nodes in the path excluding source and the destination node.

3. Destination node chooses highest PTF to acknowledge back to Source node with RREP (Route Reply) Message.

4. Number of RREP to Source node from Destination node is decided based on BACKUP_PATHS parameter in RREQ message.

4.5 Message Transmission Module

1. Message Transmission between Source and Remote Destination (Uses TCP Protocol).

2. Message is transmitted using optimal path with highest PTF

3. Update Trust Factor based on Transmission Status for each node participating in data transmission.

5 SYSTEM REQUIREMENTS

5.1. Hardware Requirements

1. Processor: Intel Pentium dual core
2. Memory: 2GB RAM 100 GB ROM
3. Any other devices: 3-5 computers

5.2. Software Requirements

1. Operating system: windows
2. Programming language: C sharp
3. Drivers: Visual studio.net (framework 4.0 or above)

6. SYSTEM DESIGN DETAILS

1. SYSTEM ARCHITECTURE

Architecture focuses on looking at the system as a combination of many different components, and how they interact with each other to produce the desired result. The focus is on identifying components or subsystems and how they connect. In other words, focus is on what major components are needed.

2. ACTIVITY DIAGRAM

Activity diagram describes the flow of control in a system. So, it consists of activities and links. The flow can be sequential, concurrent or branched. Activities are nothing

but the functions of a system. Number of activity diagrams are prepared to capture the entire flow in a system. Activity diagrams are used to visualize the flow of controls in a system. This is prepared to have an idea of how the system will work when executed.

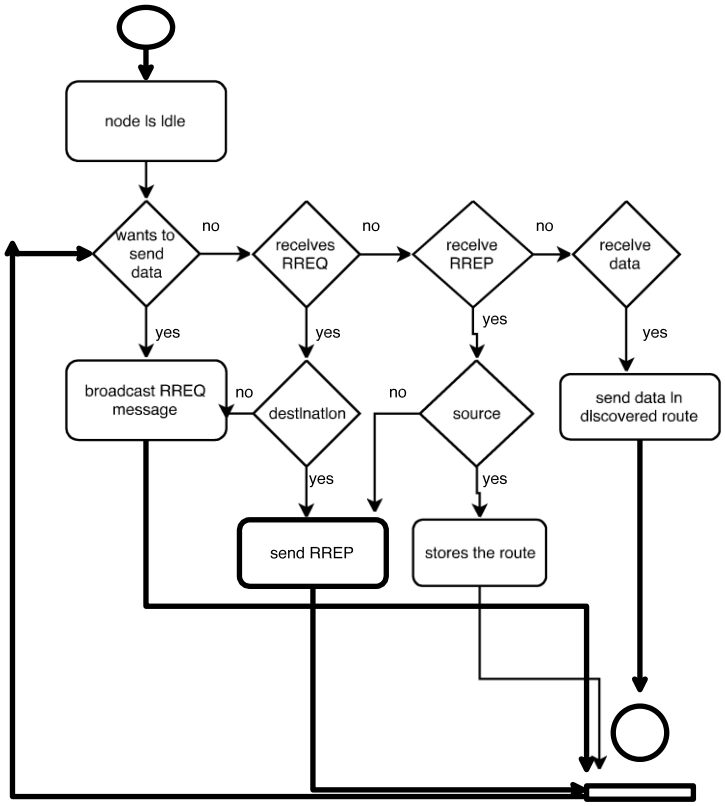

Fig-2 : Activity diagram

7. FINAL PRODUCTS

Service Log provides details about Route Request Message which contains Serviceid, TMin ,TCum ,NHMax Backup Paths and ipDetails.

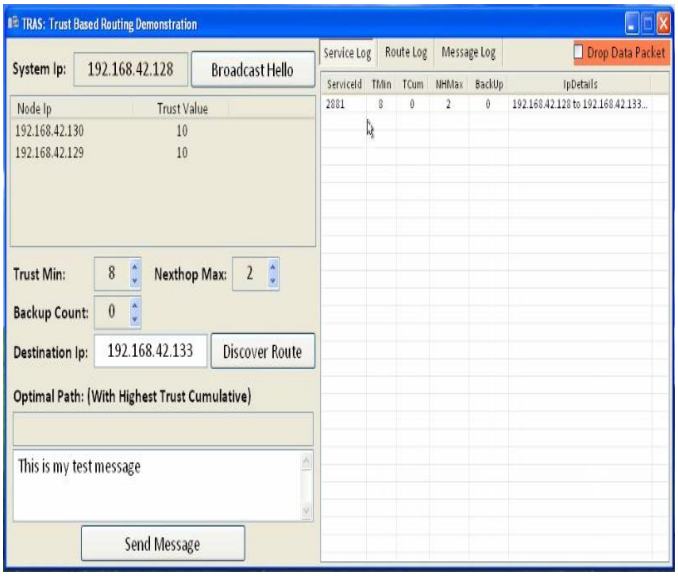

Fig-3: Service Log

Route Log provides the path through which the data packet is routed. It contains Serviceid along with the IP Address of the nodes that are participating in the Transmission.

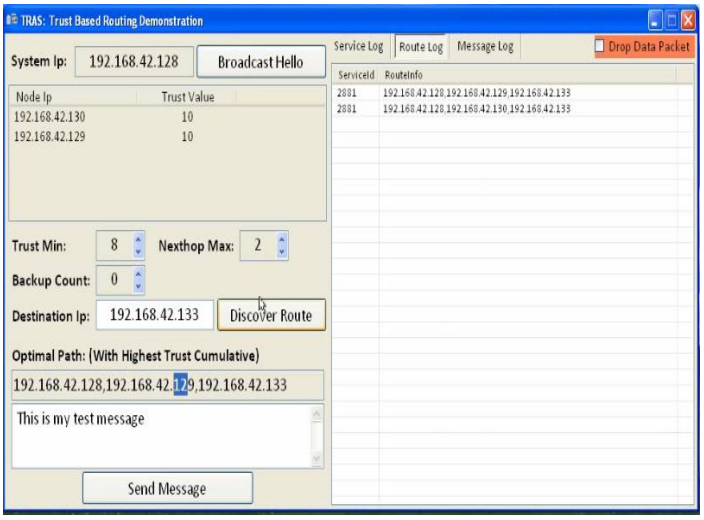

Fig-4: Route Log

Message Log contains MessageId along with From IP and to IP.

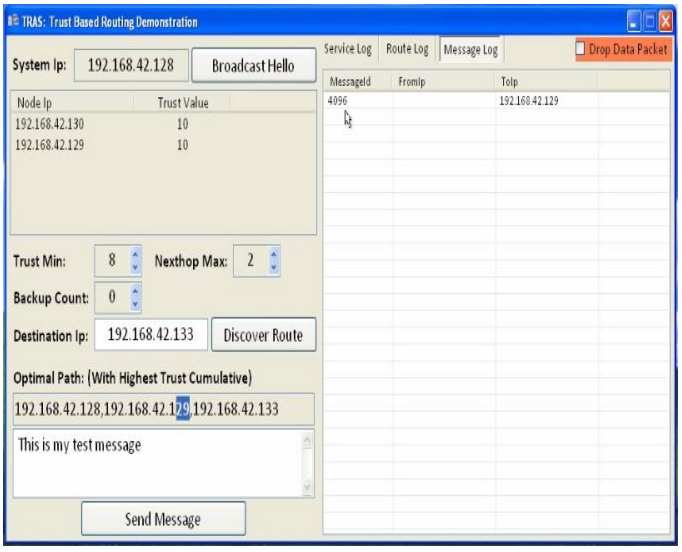

Fig-5: Message Log

8. CONCLUSION AND FUTURE ENHANCEMENTS

In this paper, a trust-based routing protocol for ad hoc and sensor networks, TRAS, was presented. Trust of discovered multi-hop paths between the source and destination nodes is an important component towards achieving enhanced security in communication. The trust factor is increased when nodes participate successfully during the data transmission process by using an acknowledgement mechanism. Currently the protocol operates based on a reward model and does not directly penalize nodes that do not participate in the data transmission process or are malicious in the process. This is an issue that we plan to further investigate to enhance the process.

REFERENCES

[1] Imad Jawhar, Farhan Mohammed, Jameela Al Jaroodi, and Nader Mohamed, IEEE International Conference on Intelligent Data and Security, United Arab Emirates University, Al Ain. UAE, 2016.

[2] Z. Liu, A.W. Joy and R.A. Thompson, A Dynamic Trust Model for Mobile Ad Hoc Networks,Proc. of IEEE International Workshop on Future Trends of Distributed Computing Systems, 2010.

[3] H. Chuanhe, C. Yong, S. Wenming and Z. Hao, "A Trusted Routing Protocol for Wireless Mobile Ad hoc Networks," 2009.

[4] S. Hadim, J. Al-Jaroodi and N. Mohammed, Middleware Issues and Approaches for Mobile Ad Hoc Networks, in proc. of IEEE Consumer Communications Networking Conference (CCNC 2006), Las Vegas, Nevada, January 2006.

[5] K. Sundaresan, V. Anantharaman, H-Y, Hsieh and R. Sivakumar, A reliable transport protocol for ad hoc networks, IEEE Transactions on Mobile Computing, 4(6)588-603, Nov/Dec 2005.

[6] C. E. Perkins, Ad Hoc Networking, Addison-Wesley, Upper Saddle River, NJ, USA, 2001.