IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 2, 2015, Page.893-898, ISSN: 2347–8586

Distributed Client Tracker in Manet

[1]G.Prabhakaran, [2]P.Sivakumar
[1]Student, [2]Assistant Professor
Department of CSE,
EBET Group of Institutions, Kangayam, India
prabhucse72@gmail.com, ps.cse@ebet.edu.in

Abstract - Mobile adhoc networks (MANETs) are ideal for situations where a fixed infrastructure is unavailable or infeasible. This limitation makes MANETs unsuitable for applications such as crisis management and battlefield communications. In battlefield team members might need to work in groups or scattered in the terrain. In such terrain, intergroup communication is crucial to the team collaboration. To address this weakness, I introduce in this paper a new class of adhoc network called SAODV. Unlike conventional networks, SAODV protocol is used for the clients in the terrain, and organizing themselves into a suitable network topology to ensure good connectivity for both intra- and intergroup communications. I propose a distributed client tracking solution to deal with the dynamic nature of client mobility and present techniques for dynamic topology adaptation in accordance with the mobility pattern of the clients. Simulation results indicate that AMMNET is robust against network partitioning and capable of providing high relay throughput for the mobile clients.

Index terms*- MANET, AODV, AMMNET,SAODV.*

I. INTRODUCTION

Ad hoc wireless networks are interconnected sets of mobile nodes that are self-organizing, self-healing, survivable, and instantaneously available, without any need for prior infrastructure. Since Internet Protocol (IP) suite is now recognized as the universal interface or “glue” for interconnecting dissimilar networks, an IP-based ad hoc network has the potential to solve the interoperability problems faced by various conventional stovepipe networks that are designed for specific usage cases. A multi-hop mesh network can be defined as a communications network that has two or more paths to any node, providing multiple ways to route data and control information between nodes by “hopping” from node to node until a connection can be established. Mobile mesh networks enable continuous efficient updates of connections to reconfigure around blocked or changed paths. The need for and value of autonomous mobile mesh networks for broadband applications is described later. This is followed by an overview of technical challenges that need to be addressed in designing autonomous mobile mesh networks and for providing useful multimedia peer-to-peer services over such networks. Emphasis is placed on describing generic system level challenges rather than on specific solutions for component subsystems, some of which are only beginning to evolve.

A.OBJECTIVE

As autonomous mobile users move about in a MANET, the network topology may change rapidly and unpredictably over time and portions of the network may intermittently become partitioned. This condition is undesirable, particularly for mission-critical applications such as crisis management and battlefield communications.

II. RELATED WORK

“A Survey on Intrusion Detection in Mobile Ad Hoc Networks” by Tiranuch Anantvalee, Jie Wu, Florida Atlantic University, Boca Raton, FL 33428.An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself. Accordingly, the study of the defence to such attacks should be explored as well. The current IDS techniques on wired networks cannot be applied directly to MANETs. Many intrusion detection systems have been proposed to suit the characteristics of MANET. “A Secure On-Demand Routing Protocol for Ad Hoc Networks” by YIH-CHUN HU and ADRIAN PERRIG and DAVID B. JOHNSON. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. They can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost.

This paper has presented the design and evaluation of Ariadne, a new secure ad hoc network routing protocol. Ariadne provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptographic operations. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" by Hu, Yih-Chun, Adrian Perrig, and Dave Johnson. Ariadne new network routing protocol design and evaluation provided a safe technology. Ariadne node is compromised and provides protection against arbitrary active attacks and not just relying on efficient symmetric cryptographic operations. Ariadne has dynamic requiring the need for discovering routes between nodes. The design is based on the basic operation of the DSR protocol. "Dynamic Source Routing in Ad Hoc Wireless Networks" by David B. Johnson David A. Maltz. This paper has presented a protocol for routing packets between wireless mobile hosts in an ad hoc network. Unlike routing protocols using distance vector or link state algorithms, our protocol uses dynamic source routing which adapts quickly to routing changes when host movement is requent, yet requires little or no overhead during periods in which hosts move less frequently.

III. PROJECT DESCRIPTION

A.PROBLEM DEFINITION

Similar to stationary wireless mesh networks, an AMMNET is a mesh-based infrastructure that forwards data for mobile clients as shown in Figure 3.1. A client can connect to any nearby mesh node, which helps relay data to the destination mesh node via multi-hop for-warding. Like stationary wireless mesh networks, where routers are deployed in fixed locations, routers in an AMMNET can forward data for mobile clients along the routing paths built by any existing adhoc routing protocols, e.g., AODV.

B.METHODOLOGY

MODULES

1. AMMNET Framework
2. Distributed Client Tracking in AMMNET
3. Topology Optimization
4. Performance Evaluation

C. *MODULE EXPLANATION*

AMMNET FRAMEWORK

The topology adaptation of an AMMNET is illustrated in **1.**The mesh clients initially concentrate in one group.

2. The mesh clients move northwards and split into two groups.

3. The same mesh clients now move and form three groups.

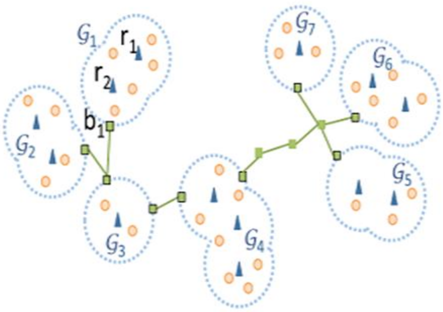


Figure 1 AMMNET Framework

In the performance evaluation of a protocol for an ad hoc network , the protocol should be tested under realistic conditions including data traffic models, and realistic movements of the mobile users. These movements are independent of each other. To know this, the detection of beacon messages transmitted from the clients is important. Two challenges in designing AMMNET are, i) the mesh clients do not have knowledge of their locations and

ii)the topology adaptation needs to be based on a highly efficient distributed computing technique to keep up with the dynamic movement of the mobile users. Partition and its topology adaptation. I classify the works related to AMMNET into three categories
1) Stationary Wireless Mesh Networks: AMMNET is a new type of mesh networks, but supports dynamic topology adaptation.
2) Sensor Covering: The techniques for sensor covering are related to the design of covering mobile clients in AMMNET.
3) Location Tracking: Tracking mobile clients in AMMNET is an application of location tracking.

DISTRIBUTED CLIENT TRACKING IN AMMNET

Networking is a distributed application architecture that partitions tasks or work, the mobility of the mesh clients is confined to the fixed area serviced by a standard wireless mesh network due to the stationary mesh nodes. In particular, an AMMNET tries to prevent network partitioning to ensure connectivity for all its users. This property makes AMMNET a highly robust MANET.

Achieves performance superior to existing protocols in terms of energy efficiency, packet delivery ratio (PDR), and latency. The mobile mesh nodes adapt their topology accordingly to archive full connectivity for all the mesh clients.

TOPOLOGY OPTIMIZATION

The clients in the coverage region of particular router can move from one location to another location. According to client’s mobility, the topology is set and routing is performed. Before communication we need to adapt the topology. The topology adaptation can be classified into two methods.
i) Local Adaptation.
ii) Global Adaptation

LOCAL ADAPTATION

Among many topologies the star topology provides shorter rely paths therefore it requires only few no of intergroup routers. Here, bridge routers exchange their location information and perform local adaptation.

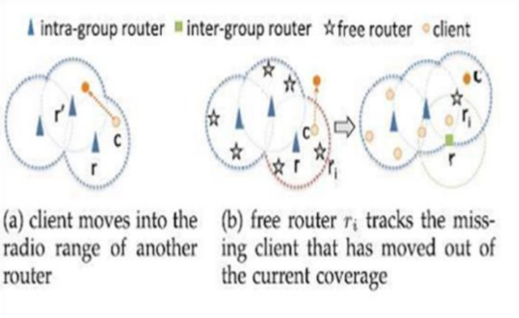
GLOBAL ADAPTATION

Local topology adaptation provides local optimization. It is desirable to also perform global topology adaptation to achieve global optimality. This method provides better overall end-to-end delay and free up intergroup routers for subsequent local adaptation. In ideal case AMMNET use few intergroup routers as possible to minimize the number of mobile routers required and deliver good end to-end delay for the application.

D. PERFORMANCE EVALUATION

Generally, the conventional mobile ad-hoc network suffer from network partitioning, this problem was solved in the AMMNET. It supports both intra-routing and inter-routing. Here, the mobile mesh routers of an AMMNET track the users and dynamically adapt the network topology and perform routing. It simply forwards the date from source to destination via multiple hops. This infrastructure provides full connectivity without need of high cost of network coverage. AMMNET does not consider that, whether the routing path is the one, which is shortest distance between the source-destination pair. We let each MANET user act as a mobile router, which can transmit/receive its own data and also forward data for other users. Each router has been reconfigured after each topology adoption.

E. SYSTEM ARCHITECTURE



(a) client moves into the radio range of another router

(b) free router r_i tracks the missing client that has moved out of the current coverage

Figure 2: System Architecture

IV. SOFTWARE SPECIFICATION

A.NETWORK SIMULATION

In communication and computer network research, network simulation is a technique where a program models the behaviour of a network either by calculating the interaction between the different network entities (host/routers, data links, packets, etc) using mathematical formulas, or actually capturing and playing back observations from a production network.

The behaviour of the network and the various applications and services it supports can then be observed in a test lab, Various Attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions. When a simulation program is used in conjunction with live applications and services in order to observe end-to-end performance to the user desktop, this technique is also referred to as network emulation.

B.NETWORK SIMULATOR

A network simulator is a piece of software or hardware that predicts the behaviour of a network, without an actual network being present. The network simulator is the program in charge of calculating how the network would behave. Such software may be distributed in source form (software) or packaged in the form of a dedicated hardware appliance. Users can then customize the simulator to fulfil their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as IPv4, IPv6, UDP, and TCP.

C. USES OF NETWORK SIMULATORS

Network Simulators serve a variety of needs. Compared to the cost and time involved in setting up an entire test bed containing multiple networked computers, routers and data links, network simulators are relatively fats and inexpensive. They allow engineers to test scenarios that might be particularly difficult or expensive to emulate using real hardware – for instance, simulating the effects of a sudden burst in traffic or a DoS attack on a network service.

Networking simulators are particularly useful in allowing designers to test new networking protocols or changes to existing protocols in a controlled and reproducible environment. Network simulators, as the name suggests are used by researchers, developers and QA to design various kinds of networks, simulate and then analyze the effect of various kinds of networks, simulate and then analyze the effect of various parameters on the network performance.

A typical network simulator encompasses a wide range of networking technologies and helps the users to build complex networks from basic building blocks like variety of nodes and links. With the help of simulators one can design hierarchical networks using various types of nodes like computers, hubs, bridges, routers, optical cross-connects, multicast router, mobile units, MSAUs etc.,

V. SYSTEM DESCRIPTION

A.DEVELOPING METHODOLOGIES

LANGUAGE

Tcl (Tool Command Language) is a very powerful but easy to learn dynamic programming language, suitable for a very wide range of uses, including web and desktop applications, networking, administration, testing and many more. Open source and business-friendly, Tcl is a mature yet evolving language that is truly cross platform, easily deployed and highly extensible.

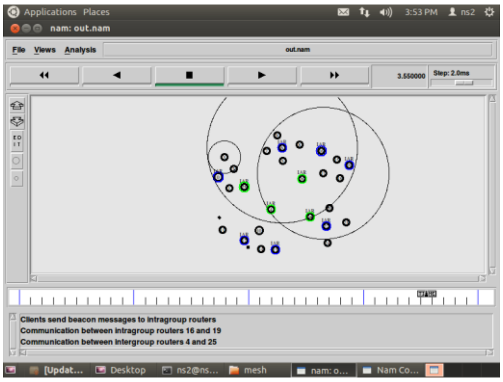
B.ALGORITHM (OR) PROTOCOL USED

ALGORITHM

Intragroup Routers: A mesh node is an intragroup router if it detects at least one client within its radio range and is in charge of monitoring the movement of clients in its range. Intragroup routers that monitor the same group of clients can communicate with each other via multihop routing. For example, routers r1 and r2 in Figure 2 is intragroup routers that monitor group G1. A mesh node is an intergroup router. If it plays the role of a relay node helping to interconnect different groups. For each group, I designate at least one intergroup router that can communicate with any intragroup routers of that group via multihop forwarding as the bridge router, for example, router b1 for group G1 free routers.
A mesh node is a free router if it is neither an intragroup router nor an intergroup router.
Algorithm1: Distributed Client Tracking for Router.
Algorithm2: Topology Adaptation (initiated by router).
Algorithm3: Hierarchical Star Topology Construction

VI. RESULTS

Node is recovered by sending a beacon message to the failure node and the coverage area can be optimized for better communication.



Clients send beacon messages to intragroup routers
Communication between intragroup routers 16 and 19
Communication between intergroup routers 4 and 25

Figure 3: Nodes are recover by SAODV

Failure node is dropped from the network.

VII. CONCLUSION AND FUTURE ENHANCEMENT

We conducted extensive simulation study to assess the effectiveness of AMMNET. The results confirm that the proposed distributed topology adaptation scheme based on autonomous mobile mesh routers is almost as effective as a hypothetical centralized technique with complete knowledge of the locations of the mobile clients. The simulation results also indicate that AMMNET is scalable with the number of users. The required number of mobile mesh nodes does not increase with increases in the user population. Although an excessively large number of user groups may affect the performance of AMMNET, the number of user groups is typically very small relative to the number of users for most applications and AMMNET is effective for most practical scenarios. The potential for enhanced network security, and also acknowledged the complexity of the encryption methods. Accepting and distributing them to the nodes of the network is possible to reduce the need for energy consumption.

REFERENCES

[1]. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, “Which wireless technology for industrial wireless sensor networks? The development of OCARI technol,”IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2]. R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” inLecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3]. R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc networks: A survey,” inProc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4]. T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: SpringerVerlag, 2008.

[5]. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6]. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, “Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks,”IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7]. V.C.Gungor and G.P.Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approach,”IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, “SEAD: Secure efficient distance vectorrouting for mobile wireless ad hoc networks,” inProc. 4th IEEE Workshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9]. Y. Hu, A. Perrig, and D. Johnson, “ARIADNE: A secure on-demand routing protocol for ad hoc networks,” inProc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10]. G. Jayakumar and G. Gopinath, “Ad hocmobile wireless networks routing protocol—A review,” J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.