JOURNAL OF COMPUTATION IN
BIOSCIENCES AND ENGINEERING

Journal homepage: http://scienceq.org/Journals/JCLS.php

Article Open Access

Secured Unicast Routing using Cross layer design in Wireless Mobile Ad Hoc Networks

N Kirubakaran[1] and A.Kathirvel[2*]
[1] Department of Computer Science Engg. St. Peter's Univeristy, Sankar Nagar,Avadi, chennai, India
[2] Department of Computer Science Engg. Misrimal Navajee Munoth Jain Engineering College, Chennai, India,
*Corresponding author: A.Kathirvel, E-mail: ayyakathir@rediffmail.com
Received: February 25, 2017, Accepted: March 27, 2017, Published: March 27, 2017.

ABSTRACT:

A wireless mobile ad hoc network is a dynamic wireless network with the engagement of cooperative nodes with a infrastructure less networks. Multicasting routing is intended for group communication that supports the dissemination of information from a sender to all the receivers in a group. Problems in ad hoc networks are the scarcity of bandwidth, short lifetime of the nodes due to power constraints, dynamic topology caused by the mobility of nodes. We would like to provide solution for the above problem using the cross layer approach. In a cross-layer design, where the medium access control layer functionality and the network layer functionality are performed by a single integrated layer. The basic design philosophy behind the multicast routing part of the architecture is to establish and maintain an active multicast tree surrounded by a passive mesh within a wireless mobile ad hoc network. Thus, the multicast backbone is a condensed passive mesh woven around a highly pruned tree. Although tree-based and mesh-based multicasting techniques have been used separately in existing multicasting architectures, the novelty in this study is the integration and reengineering of the tree and mesh structures to make them highly energy efficient and robust for real-time data multicasting in mobile ad hoc networks. Energy efficiency is achieved by enabling the nodes to switch to sleep mode frequently and by eliminating most of the redundant data receptions. Extensive simulation studies using Network Simulator helps to study the proposed solution soundness and prove the robustness of the system.

Keywords: *Wireless network Computing, Privacy Preservation, Data,Tiered Blind and Anonymous Hierarchical Identity Based Encryption (TBAHIBE) and Location Based Keyword Query Search (LBKQS), Electronic Health Record (EHR).*

.

INTRODUCTION

Mobile ad hoc networks (MANET) are self-creating, self-administering and self-organizing entities [1 -2]. Thus a set of self-motivated mobile wireless users is able to dynamically exchange data among themselves even in the absence of a predetermined infrastructure and controller. Each user of mobile ad hoc network also acts as a router allowing other users to communicate through their mobile communication device. The communication range of each device is limited; therefore, at any given time a user can exchange packets only with any one of the devices in its transmitting or receiving range.

Unlike the conventional cellular networks that rely on extensive infrastructure to support mobility, a MANET does not need expensive base stations and wired infrastructure [3]. These features are important for potential use in a wide variety of disparate situations [4]. Such situations include battlefield communications and disposable sensors, which are dropped from high altitudes and are dispersed on the ground for hazardous materials detection [5]. Civilian applications include emergency situations such as responses to hurricane, tsunami, earthquake, and terrorism. Another interesting example is the case, where a set of mobile vehicles on the highway form an ad hoc network of their own in order to provide vehicular traffic management. Security provisioning in wireless ad hoc networks plays an integral part in determining the success of network centric warfare as envisioned for future military operations. Thus, security is an important issue for these mission-critical applications, is discussed in next section. Extensive simulation studies using Network Simulator helps to study the proposed solution soundness and prove the robustness of the system [6].

In this paper we will explain, our proposed CLUS model. The rest of the paper is organized as follows: Section 2 provides application of ad hoc networks; Section 3 Overview of Issue and challenges of the proposed model; CLUS model is given in section 4. Section 5 we explore related work and Section 6 draws up conclusions.

2. Application of Ad Hoc Networks

Its Applications are listed in details are given below,

- Safety applications
  - Lane change warning
  - Co-operative Collision Warning
  - Approaching emergency vehicle
  - Rollover warning
  - Intersection Collision Warning
- Tactical networks
  - Military communication and operations
  - Automated battlefields
- Emergency services • Search and rescue operations
  - Disaster recovery
  - Replacement of fixed infrastructure in case of environmental
- disasters
  - Policing and fire fighting
  - Supporting doctors and nurses in hospitals
- Commercial and civilian
  - E-commerce: electronic payments anytime and anywhere
- environments

- Business: dynamic database access, mobile offices
- Vehicular services: road or accident guidance, transmission of

- road and weather conditions, taxi cab network, inter-vehicle networks
  - Sports stadiums, trade fairs, shopping malls
  - Networks of visitors at airports
- Home and enterprise
  - Home/office wireless networking
- networking Conferences, meeting rooms
  - Personal area networks (PAN), Personal networks (PN)
  - Networks at construction sites
- Education Universities and campus settings
  - Virtual classrooms
  - Ad hoc communications during meetings or lectures
- Entertainment Multi-user games
  - Wireless P2P networking
  - Outdoor Internet access
  - Robotic pets
  - Theme parks
- Sensor networks
  - Home applications: smart sensors and actuators embedded in consumer electronics
  - Body area networks (BAN)
  - Data tracking of environmental conditions, animal
- movements, chemical/biological detection
- Context aware services
  - Follow-on services: call-forwarding, mobile workspace
  - Information services: location specific services, time
- dependent services
  - Infotainment: touristic information
- Coverage extension
  - Extending cellular network access
  - Linking up with the Internet, intranets, etc.
- Non Safety applications
  - Coupling/Decoupling
  - Inter vehicle communication
  - Parking Lot payment

3. Issues & Challenging

Issues of an Ideal Routing Protocol

- Fully distributed
- Adaptive to frequent topology changes
- Minimum connection setup time is desired
- Less propagation control overhead
- Loop free and free from stale routes
- Packet collision must seldom happen
- Converge to optimal route quickly
- Optimally use scarce resource – Bandwidth, computing power, memory, and battery
- Remote parts of the network must not cause updates in the topology information maintained by this node
- Provide quality of service and support for time sensitive traffic

Challenging Constraints in Designing a Routing Protocol

- Mobility
  - frequent path breaks
  - packet collisions
  - stale routing information
  - difficulty in resource reservation
- Bandwidth Constraint
  - shared channel
  - only a fraction of total bandwidth is available for every node
- Resource Constraints
  - Battery Power
  - Computing capability
  - buffer storage
- Error-prone shared broadcast radio channel
  - Bit Error Rate and path loss is high
  - Signal to Noise Ratio is less

4. Proposed Model

Wireless Mobile Ad hoc Networks (WMN) provide wireless mobile communication capability to satisfy a need of a temporary nature and without the existence of any well-defined infrastructure. Protecting the network layer operation from malicious attacks is an important and challenging issue in both wired and wireless networks and the issue becomes even more challenging in the case of WMN. In this paper, we propose a frame work Cross Layer Umpiring System (CLUS) that provides security for routing and data forwarding operations. In our system, each node's behavior from source to destination is closely monitored by a set of three umpires. If any misbehavior is noticed, CLUS flag off the guilty node from the circuit. We have proposed three enhancements to the basic ETUS such as Link status, Token status and Battery status as shown in the Fig. 1.

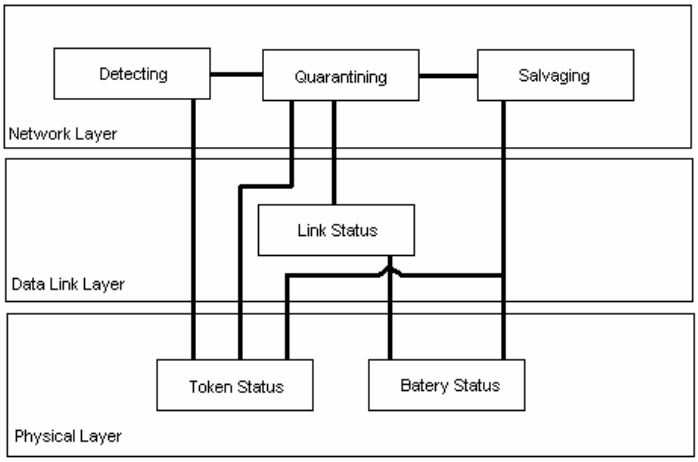

Fig. 1 Frame work of CLUS

Protocols have need of correct information of the link status between neighboring mobile nodes. In the token status misbehaving nodes, token status is changed. Battery Life status is helpful to choose good battery strength nodes. The model with these three enhancements is called CLUS. We have implemented CLUS using AODV protocol. Extensive investigation studies using simulator [6] establish the soundness and robustness of the proposal. Work in progress next paper result will be published.

5. Related Works

The approaches for detecting packet dropping attacks can be categorized as three classes: multipath forwarding approach, neighbor monitoring approach, and acknowledgment approach [1

-4].

A team of robots are deployed to accomplish a task while maintaining a viable ad-hoc network capable of supporting data transmissions necessary for task fulfillment. Solving this problem necessitates: 1) estimation of the wireless propagation environment to identify viable point-to-point communication links; 2) determination of end-to-end routes to support data traffic; and 3) motion control algorithms to navigate through spatial configurations that guarantee required minimum levels of service [7].

One such uncertainty is wireless communication itself which assumes complex spatial and temporal dynamics. For dependable and predictable performance, therefore, link estimation has become a basic element of wireless network routing. Several approaches using broadcast beacons and/or unicast MAC feedback have been proposed in the past years, but there is still no systematic characterization of the drawbacks and sources of errors in beacon-based link estimation in low-power wireless networks, which leads to ad hoc usage of beacons in routing [8].

Many defenses based on spatial variability of wireless channels exist, but depend either on detailed, multi-tap channel estimation something not exposed on commodity 802.11 devices-or valid RSSI observations from multiple trusted sources, e.g., corporate access points-something not directly available in ad hoc and delay-tolerant networks with potentially malicious neighbors [9].

6. CONCLUSION

A mobile Ad-hoc network provides the mobility of nodes which is so helpful in any emergency situations. However, if security accidents and packet loss occurs, ruinous economic damages are inevitable. Our project proposed a new model that focuses on detection on malicious node and avoids them to increase the performance. Proposed method provides how we decrease the traffic and rate of vulnerability in the system using CLUS. Implementing the same concept in wireless sensor networks which may be helpful in real-time. Work in progress.

REFERENCES

1. Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, “ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks”, International Journal of Communication Networks and Distributed Systems, Vol. 7, No. 1 / 2, pp. 153 – 187, 2011.
2. Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, “ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks”, International Journal of Network Management, Vol. 21, No. 5, pp. 341 – 359, 2011.
3. B. Xiao, B. Yu, and C. Gao, “Chemas: Identify Suspect Nodes in Selective Forwarding Attacks,” Journal Parallel and Distributed Computing, Vol. 67, No. 11, 2007.
4. Kathirvel A Srinivasan R and Mohanambal K, “Monograph: Umpiring Security Model & Performance Imporovement on MANETS”, LAP Lambert Academic Publishing GmbH & Co.Germany. Europe. 2011. ISBN 978-3-8473-0621-9
5. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, “Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks”, Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.
6. A. Kathirvel, “Introduction to GloMoSim”, LAP Lambert Academic Publishing GmbH & Co.Germany. Europe. 2011. ISBN 978-3-8473-2397-6.
7. Fink, J.; Ribeiro, A.; Kumar, “Robust Control of Mobility and Communications in Autonomous Robot Teams”, IEEE Journals & Magazines, Vol. 1, pp.290 - 309, 2013.
8. Zhang, Hongwei,” Experimental analysis of link estimation methods in low power wireless networks”, TUP Journals & Magazines, Vol. 16, No. 5, pp. 539 - 552, 2011.
9. Yue Liu; Bild, D.R.; Dick, R.P.; Mao, Z.M.; Wallach, D.S.,” A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities”, IEEE Transactions on Mobile Computing, Vol. 14, No. 11, pp. 2376 - 2391, 2015.

Citation: A.Kathirvel, *et al*. (2017). Secured Unicast Routing using Cross layer design in Wireless Mobile Ad Hoc Networks. J. of Computation in Biosciences and Engineering. V3I3. DOI: 10.15297/JCLS.V3I3.03