Efficiency Improvement in PUMA Protocol Using A Network Simulator NS – 2.35 and Get Secure PUMA in Mobile Ad – Hoc Network

Vishalkumar Hansrajbhai Kanani

Department of Information Technology (M.E.)

Parul Institute of Engineering & Technology

At – Post Limda, Waghodiya Road, Vadodara

Gujarat Technological University (Ahmadabad)

Abstract

An Ad hoc Network consists of a set of autonomous mobile nodes that communicates via multi-hop wireless communication in an infrastructure less environment. It is an autonomous system in which mobile nodes connected by wireless links are free to move randomly and often act as routers at the same time. Ad hoc networks have become increasingly relevant in recent years due to their potential applications in military battlefield, emergency disaster relief, vehicular communications etc.

In ad hoc networks, nodes communicate with each other by way of radio signals, which are broadcast in nature. Broadcast is a unique case of multicast, wherein all nodes in the network should get the broadcast message. In ad hoc applications, collaboration and communication among a group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and resources. Multicasting is a communication process in which the transmission of message is initiated by a single user and the message is received by one or more end users of the network. Multicasting in wired and wireless networks has been advantageous and used as a vital technology in many applications such as audio/ video conferencing, corporate communications, collaborative and groupware applications, stock quotes, distribution of software, news etc. Under multicast communications, a single stream of data can be shared with multiple recipients and data is only duplicated when required. Main purpose of multicasting is to provide multiple packets to multiple receivers using bandwidth and energy efficiently.

Introduction

Mobile networking is one of the most important technologies supporting pervasive computing. During the last decade, advances in both hardware and software techniques have resulted in mobile hosts and wireless networking common and miscellaneous. Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other: [6]

1) Infrastructure. Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind

of wireless networks are GSM, UMTS, WLL, WLAN, etc.

2) Infrastructure less. As to infrastructure less approach, the mobile wireless network is commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system.

In this report, we describes the fundamental problems of ad hoc networking by giving its related research background including the concept, features, status, and applications of MANET. Some of the technical challenges MANET poses are also presented. Some of the key research issues for adhoc networking technology are discussed in details that are expected to promote the development and accelerate the commercial applications of the MANET technology. [9]

The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols.

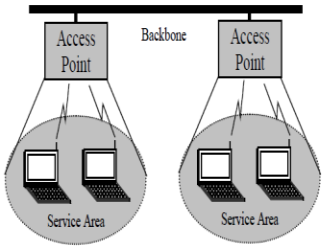
MANET Concept

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network, including:

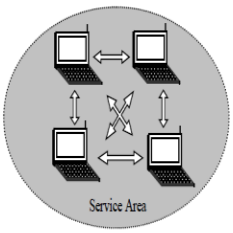
1) Peer-to-Peer. Communication between two nodes which are within one hop. Network traffic (Bps) is usually consistent.

2) Remote-to-Remote. Communication between two nodes beyond a single hop, but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.

3) Dynamic Traffic. This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.



(a) Infrastructure-based wireless network



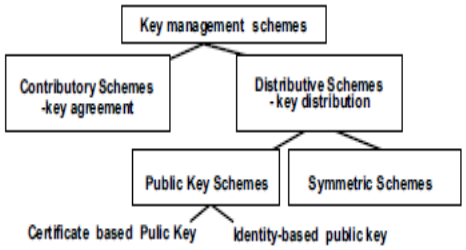
(b) Ad hoc wireless network

Figure-1: Types of Wireless network [9]

PUMA

PUMA (Protocol for Unified Multicasting through Announcement) [4] does not require any unicast routing protocol to operate, or the pre-assignment of cores to groups. The section below shows PUMA operation in detail. PUMA derives from its use of very simple signaling (multicast announcements) to accomplish all the functions needed in the creation and maintenance of a multicast routing structure in a MANET. Multicast announcements are used to elect cores dynamically, determine the routes for sources outside a multicast group to unicast multicast data packets towards the group, join and leave the mesh of a group, and maintain the mesh of the group. PUMA protocol is advantageous due to its high packet delivery ratio and limited congestion [4]. The comparison of multicasting protocols is shown in table 1.

Key management



Classification of Key Management schemes

Contributory Schemes (Key Agreement):-

Contributory key agreement, in which each node contributes an input to establish a common secret (which is a function of all nodes' inputs) through successive pair wise message exchanges among the nodes in a secure manner. D-H (Diffie-Hellman), ING (Ingemarsson, Tang and Wong CKDS), B-H (Burmester and Desmedt) and CLIQ follow contributory approach. The contributory approach of no trusted third parties and previously exchanged security credentials fits well for both single security domain and multiple security domain scenarios. However, none of the contributory schemes are good candidates for key management in wireless ad hoc networks. The main deficiencies of Diffie-Hellman and ING are missing authentication. B-H and CLIQ have an inherent survivability problem as they require reliable multicasting. A-G (Password authenticated key agreement) is the best alternative, but exhibits limited robustness and scalability in dynamic networks.

Distributive Schemes (Key Distribution):-

Public Key Schemes: - Public key schemes involves following sub schemes:-

Partially Distributed Certificate Authority: - The scheme is suitable for planned, long term ad hoc network. This scheme is based on public key encryption. The method uses trusted offline CA and (k,n) threshold scheme to protect private key. Offline dealer assigns a valid certificate and public key to the nodes that join the network. The private key of the node is shared by k serving nodes. The serving nodes are selected randomly in the network. The new node must collect all the n partial key shares to compute the whole private key. This scheme has the following drawbacks: i) serving node must maintain public key of all other nodes in the network, which requires more memory space ii) lack of certificate revocation mechanism iii) not suitable for larger network iv) the algorithm doesn't deal with network synchronization

when split or join occurs in the network v)

	ODMRP[12]	MAODV[8]	CAMP[4]	AMRIS[1]	PUMA[4]
N/w topology	Mesh	Tree	Mesh	Tree	Mesh
Initialization approach by	Source	Source	Source & Receiver	Source	Receiver
Maintenance approach	Soft State	Hard State	Hard State	Soft State	Soft state
Dependency	No	Yes	Yes	No	No
Loop free	Yes	Yes	Yes	Yes	Yes
Flooding of control packet	Yes	Yes	No	No	No
Independent routing protocol	Yes	Yes	No	No	Yes
Periodic control message	Yes	Yes	No	Yes	Yes
Advantage	Packet delivery ratio is better due to route redundancy	Avoids sending duplicate packets to receivers Routes are on demand	Better Bandwidth allocation. Good scalability because due to no flooding	No loops. Link breaks are locally repaired. simplicity	High data delivery ratio. limited control overhead
Disadvantage	Create congestion due to high processing load	High end to end delay. High network load due to larger data & control transmission	Network convergence and control traffic growth in the presence of mobility	Waste of bandwidth. Slow rejoin scheme. increased average hop distance	No acknowledgement . no delivery validation

serving nodes may not be in contact at all times.

Table 1: Comparison of Multicasting Protocols

Fully Distributed Certificate Authority: - The scheme is based on public key encryption and is suitable for long term ad hoc network. Unlike partially distributed CA, the capability of certificate authority is distributed to all the nodes in the network. All nodes in network holds partial share of the private key. Private Key is computed by combining any k partial shares. This scheme has the following drawbacks: i) the method doesn't deal with network synchronization ii) threshold parameter k need to be larger since attacker may compromise large number of shares between share update iii) complex maintenance protocol.

Identity based key management scheme- The scheme uses set of Private Key Generation (PKG) nodes to generate public key and private key of the node. The public key of the node is generated based on node's identity. A node must contact at least k PKG nodes to obtain its private key. This scheme reduces communication and computation cost because each node would not have to create its own public key and broadcast it in the network. This scheme doesn't deal with key update. ID based public key management provides bandwidth limited than certificate based system.

Symmetric key schemes

Symmetric key systems use the common key for both encryption and decryption. This method is faster, easier to implement, and it lowers overhead on system resources. A major disadvantage of symmetric algorithm is the exchange of shared secret key between two parties. This security mechanism lacks in data authentication and integrity.

KDC (Pre-distributed group key)-The old and well-proven manual key management scheme with a Key Distribution Centre distributing symmetric keys.

Self Issued Certificates

The scheme is suitable for long term network that does not require any infrastructure. There is no centralized CA. Each node creates its own private key and certify public key to other nodes, if it has trust on that node. This scheme has the following drawbacks: i) the method doesn't deal with certificate revocation i) during initial stage, the certificate chain may not be found between all nodes in the network. iii) The system is less trusted without any trusted authority.

Secure Pebble nets

Secure pebble net is suitable for long term ad hoc network with low performance nodes. Network is partitioned into pebbles, where node with maximum weight is selected as key manager. All nodes in a pebble share a common traffic encryption key for secure communication. This scheme support group authentication and not support individual member authentication.

Conclusion

PUMA is chosen for multicast ad hoc network based on comparison of various multicasting protocols. PUMA incurs far less overhead as compare to other multicasting protocols. It has higher delivery ratios because tree based protocols have to maintain tree structure so they expend too many packets which leads to congestion.

Also one of the major problems in multicast ad hoc networks is how to manage the cryptographic keys and various security algorithms that are needed. A proper key management scheme is thus a critical factor for success of multicast ad hoc network.

Future work

Future work will mainly focus on performance analysis of PUMA protocol using a network simulator NS- 2.35.
To achieve secure PUMA in Ad hoc network, I need to have a secure multicasting after more analysis on key management schemes with various security algorithms.

References

[1] 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems
Efficient and Robust Multicast Routing in Mobile **Ad** Hoc Networks
Ravindra Vaishampayan J.J. Garcia-Luna-Aceves
Department of Computer Science, University of California Santa CNZ
ravindra@cse.ucsc.edu jj @cse.ucsc.edu
[2] This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings
Reliability and Overhead Analysis of Multicast BitTorrent Enabled Ad Hoc Network Routing
Padmini Vellore,Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John's, NL, Canada - A1B 3X5
Email: padmini.vellore@mun.ca
Email: paul@mun.ca Email: venky@mun.ca
[3] 2011 International Conference on Advanced Technologies for Communications (ATC 2011)

An efficient and message-optimal multicast routing protocol in mobile ad-hoc networks
Hai Trung Nguyen,University of Engineering and Technology,Vietnam National University
Hanoi, Vietnam
nguyen.hai@vnu.edu.vn
Dai Tho Nguyen
nguyendaitho@vnu.edu.vn

[4] J. **1.** Garcia-Luna-Aceves and E.L. Madmga, **"The** core assisted mesh protocol," ***IEEE Jurrmal on Selected Arear in Communications Special Issue on Ad-Hoc Neworkr,*** **vol.** 17, **no.** 8, pp. **1380-1394,** August 1999.

[5] **S.J. Lee,** M. Gerla, and Chian, "Ondemand multicast routing pmtocol," in ***Pmceedings*** of ***WCNC,*** September 1999.

[6] S.J. **Lee,** W. **Su,** 1. **Hsu,** M. Geda. and R. Bagrodia **"A** performance comparison study of ***ad*** hoc wireless multicast pmtocols:' in ***Pmceedings*** of ***IEEE INFOCOM.*** *Tel* ***Aviv, Israel,*** March ZWO.

[7] **J.** Xie snd R.R. Talpade, **A.** McAuley, and M. Liu, **"Ammute:** Ad hoc multicast muting protocol," ***Mobile Nefworkr and Applications (MONETJ,*** December 2002.

[8] R. Vaishampayan and J.J. Garcia-Luna-Aceves, "Robust multicasting in ad hoc networks using trees(romant)," in *International Journal on Wirless and Mobile Computing(IJWMC)*, 2004.
[9] R. Vaishampayan and J.J. Garcia-Luna-Aceves, "Protocol for unified multicasting through announcements (puma)," in *Proceedings of the 1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, October 2004.

[10] P. Vellore, P. Gillard, and R. Venkatesan, "Probability distribution of multi-hop multipath connection in a random network," in *IEEE GLOBECOM '09: Proceedings of the 2009 IEEE Global Communications Conference*, December 2009.

[11] P. Vellore, P. Gillard, and R. Venkatesan, "MBEAN: Multicasting in BitTorrent enabled ad hoc networks," *International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 2, pp. 929–934, June 2005.