The Reliable Broadcasting in Mobile Ad-Hoc Networks

[1]D Sunitha, [2]Ch. Raja Jacob
[1,2]Dept. of CSE, Nova College of Engineering & Tech, Jangareddy Gudem, AP, India

Abstract
It will guarantee to deliver the messages from different sources to all the nodes of the network. The nodes are mobile and can move from one place to another. The solution does not require the nodes to know the network size, its diameter and number of nodes in the network. The only information a node has its identity (IP Address) and its position. On average, only a subset of nodes transmits and they transmit only once to achieve reliable broadcasting.
The algorithm will calculate the relative position of the nodes with respect to the broadcasting source node. The nodes that are farthest from the source node will rebroadcast and this will minimize the number of rebroadcasts made by the intermediate nodes and will reduce the delay latency. The proposed algorithm will adapt itself dynamically to the number of concurrent broadcasts and will give the least finish time for any particular broadcast. It will be contention free, energy efficient and collision free. The reliable broadcasting algorithm will make this possible & the scheduling algorithm considers the relative position of the nodes with respect to the broadcast source.

Keywords
Network Nodes, Mobile Network, Ad hoc Network, Reliable Broadcasting

I. Introduction

In the wireless communication systems, there with be a need for the rapid deployment of Independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios can not rely on centralized and organized connectivity, and can be conceived as applications of mobile Ad hoc networks(MANET).
A mobile Ad hoc network(MANET) is a set of nodes communicating with each other via multi-hop wireless links. Each node can directly communicate with only those nodes that are in its communication range Intermediate nodes forward messages to the nodes that are more than are hop distance from the source. Since the nodes are mobile, the topology the network is constantly changing. The set of applications for MANET s in diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. Broadcasting is the process in which are node sends a packet to all other nodes in the network . Broadcasting is often necessary in MANET routing protocols.
Existing broadcasting methods in mobile and ad hoc networks are single source broadcasting algorithms in which only one source node can send the broadcast message to all the nodes in the network. Existing broadcasting algorithms are classified into following types.

II. Reliable Broadcasting in the Mobile

The packet radio network model is a simple and clean model that allows one to design and analyse broadcast algorithms with a reasonable amount of effort. However, since it is a high-level model, it does have some serious problems with certain scenarios in practice. For example, in reality it is not true that the transmission range of a node is the same as its interference range. Instead, the interference range of a node is usually at least twice as large as its transmission range. Not taking this into account may result in broadcasting algorithms that cannot handle certain scenarios well although efficient on paper. In fact, it is not difficult to construct examples (see [16]), where most existing protocols for broadcasting require $\Omega(n)$ rounds even in expectation when we consider the situation that the interference range is bigger than the transmission range. Thus it is necessary that algorithms for broadcasting in wireless networks consider problems due to interference. There is a limited number of papers that use a model that differentiates between the transmission range and interference range [1, 7, 8], but they assume that nodes are distributed in an ideal space so that the transmission range and interference range of every node can be specified in terms of Euclidean distance. Another serious limitation in most of the existing algorithms is the assumption that the size of the network, or at least a linear estimate of the size of the network, is available to all of the nodes in the network. Without an estimate of the size of the network it was shown in [11] that in an n node network, $\Omega(n)$ time units are required in expectation for a single message to be sent successfully, if physical carrier sensing is not available. We will use a much more general wireless communication model that recently appeared in [17]. In this work we present self-stabilizing algorithms for broadcasting and information gathering in wireless overlay networks. To keep this paper at a reasonable length, we do not give a detailed motivation for the model adopted but instead refer the interested reader to [17].Broadcasting is a basic communication primitive for wireless networks, and it has therefore been heavily studied both in the systems and in the theory community. Though broadcasting itself appears to be an easy problem, it is actually quite hard to realize in an efficient and reliable way in a mobile ad-hoc network. The main problem concerning theoretical investigations is that mobile ad-hoc networks have many features that are hard to model in a clean way. Major challenges are how to model wireless communication and how to model mobility. Here, theoretical work is still rare. So far, people in the theory area have mostly looked at static wireless systems (i.e. the wireless units are always available and do not move).Wireless communication is usually modeled using the packet radio network model. In this model, the wireless units, or nodes, are represented by a graph, and two nodes are connected by an edge if they are within transmission range of each other. Transmissions of messages interfere at a node if at least two of its neighbors transmit a message at the same time. A node can only receive a message if it does not interfere with any other message(s).

II. Ad-Hoc Network Challenges

An ad hoc network is a dynamic type of network which is both similar and very different to its parent fixed communication network. In the following we introduce the properties of an ad hoc network as a way of defining its shortcomings and to highlight its security challenges.

A. Dynamic Network

Dynamic Network have no fixed or existing network infrastructure. The network architecture is continuously changing as the network evolves. There is no preexisting or fixed architecture which handles all network tasks such as: routing security and network

management. Instead, the network infrastructure is spontaneously set up in a distributive manner. Each participating node shares the network's responsibilities. Distribution of network functionality avoids single point attacks and allows for the network to survive under harsh network circumstances. A fixed entity structure, such as a base station or central administration, is crucial for security mechanisms. A trusted third party member, which is expected in traditional networks, is similar to a fixed entity as both define security services: manage and distribute secret keying information. Therefore the absence of such a control entity introduces new opportunities for security attacks on the network.

B. Self Organized Nature

Wireless ad hoc nodes cannot rely on an off-line trusted third party meme. The security functions of the trusted third party member are distributed among the participating nodes. Each node takes responsibility for establishing and maintaining its own security and is, therefore, the centre of its own world and authority. A wireless ad hoc network is therefore referred to as a self organized network.

C. No Prior Relationships

In ad hoc networks, nodes can have no prior relationships with other nodes within the network. Prior acquaintance between nodes can be considered as pre-trust relationships between nodes. However, the ad hoc nature of these networks does not allow for these assumptions, as it cannot be assumed the secrets exist between the respective pair of nodes. If nodes can join and leave the network at random without prior trust relationships with nodes, access control becomes a difficult task for the security mechanism.

D. Multi-hop Communication Channel

Wired networks include fixed nodes and fixed wired communication lines. Wireless ad hoc networks have mobile wireless nodes(often in the form of hand held devices) and, as suggested, their communication medium is wireless. This allows for greater network availability and easy network deployment. Each node's transmission range is limited and network communication is realized through multi-hop paths. Co-operation and trust along these paths is a crucial aspect of the security mechanism and ensures successful communication. The shared wireless communication medium means that any user can participate in the network. This creates access control problems for security mechanisms as adversaries are able eavesdrop on communication or launch active attacks to alter message data.

E. Mobility

Nodes are expected to be mobile within an ad hoc network, creating a dynamic and unpredictable network environment. In certain situations the nodes mobility is not totally unsystematic and assumptions can be made in the form of mobility patterns. An example of these pattern is evident in a vehicular ad hoc network where vehicle move along fixed paths, or roads, at speeds which have a high probability of being within the local speed limit. However, nodes demonstrate random mobility within these predictions. Connectivity between nodes is sporadic. This is due to the shared, error-prone wireless medium and frequent route failures which caused by the unpredictable mobility of nodes .increased mobility can result in the multi-hop communication paths being broken and network services becoming unavailable. Security mechanisms must account for the weak connectivity and unavailability. Furthermore, due to mobility and sporadic connectivity, these mechanisms must also aim to be scalable with the changing network density.

1. Security Objectives and Services

Security mobile ad hoc networks requires certain services to be met. A security service is a made available by a protocol which ensures sufficient security for the system or the data transferred. The security objectives for mobile ad hoc networks are similar to that of fixed wired networks. The security objects are described in six categories, adapted from discussions in:

- Authentication
- Access Control
- Data Integrity
- Non-repudiation
- Availability Services

(i). Attacks

Threats or attacks upon the network come from entities. They are known as adversaries. Mobile ad hoc networks inherit all the threats of wired and wireless networks. With these networks unique characteristics, new security threats are also introduced. Before the development of security protocols, it is essential to study the attacks associated with these unique networks.

(a). Attack Characteristics

Attacks will be launched against either the vulnerable characteristics of a mobile ad hoc network or against its security mechanisms. Attacks against the security mechanism in all types of networks, including mobile ad hoc networks, include authentication and secret key sabotage. Mobile ad hoc networks have distinctive characteristics, as identified in Section . Attacks are expected to target these points of vulnerability, for example the multi-hop nature of communication routes. The attacks are classified by their different characters. The attacks, accordingly, are classified as follows:

2. Passive and Active Attacks

Security attacks can be classified by the terms active and passive [Stalling, 2002]. Passive attacks attempt to steal information from the network without altering the system resources. Examples of passive attacks include, eavesdropping attacks and traffic analysis attacks. It is difficult to detect passive attacks as they leave no traceable affect upon the system resources or network functionality. Although the results or the need for securing against these attacks may not be monitored or visibly present, it is still a priority to protect networks from these seemingly harmless attacks, particularly in a military context. Concerning this point, Bruce mentioned: "If security is too successful, or perfect then the security expenditures are seen as wasteful because success is too invisible". However, Schneier assures one that, despite the lack of visible results, the need to secure information still exists. Active attacks attempt to modify system resources or network functionality. Examples of these attacks are message modification, message replay, impersonation and denial of service attacks.

3. Insider and Outsider Attacks

Malicious nodes are not authorized participants in the network, which launch outsider attacks. Impersonation, packet insertion, and denial of service are some examples of outsider attacks. In contrast to outsider attackers, inside attackers are more difficult to defend against. Inside attacks are launched from nodes which

are authorized participants in them network. Insider attacks are common in pure mobile ad hoc network, where any user can freely join or exit. Security mechanism become vulnerable when participates are malicious and the confidentiality of keying information can be compromised. Thus, an advantage of the non-repudiation and authentication techniques, malicious insider nodes can be identified and excluded.

4. Layer Attacks

There are threats at each layer of the mobile ad hoc network communication protocol. The physical layer is vulnerable to passive and active attacks. The attacks found at the physical layer are as follows: eavesdropping; denial of service; and physical hardware alterations. Encrypting the communication links and using tamper-resistant hardware helps to protect the physical layer. However, at the data link layer adversaries can flood the communication links with unnecessary data to deplete network resources. Security mechanisms that provide authentication and non-repudiation can prevent this, as they allow invalid packets transfers to be identified. At the application layer messages are exchanged in an end-to-end manner using wireless multi-hop routes established by the network layer. The wireless multi-hop routes are invisible to the application layer. Conventional security techniques used for wired networks can be used to prevent expected attacks upon the application layer. The application layer is dependent upon the network layer to provide secure routes between the two communicating parties. The network layer provides a critical service to the mobile ad hoc network, and the routing protocol. In the context of trust and security, the provision of secure routes is one of the most vital elements for trust establishment.

III. Conclusion

Broadcasting is often necessary in MANET routing protocols. Existing broadcasting methods in mobile ad hoc networks are single source broadcasting algorithm in which only one source node can send the broadcast message to all the nodes in the network. In the wireless communication systems, there will be a need for a rapid deployment of Independent mobile users. Dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks.

References

[1] Denning, D. E.,"Encryption and Law Enforcement", Georgetown University", Computer Science Dept., Feb. 21, 1994, available by anonymous ftp from cpsr.org.

[2] Diffie, W., Hellman, M. E.,"New Directions in Cryptography", IEEE Trans. on Information Theory, IT-11:644 654, November 1976.

[3] Lacy, J., Mitchell, D., Schell, W.,"CryptoLib: Cryptography in Software", Proc. Fourth USENIX Security Workshop, October 1993.

[4] Ioannidis, J., Blaze, M.,"Architecture and Implementation of Network-Layer Security Under Unix", Proc. Fourth USENIX Security Workshop, October 1993.

[5] National Bureau of Standards,"Data Encryption Standard", FIPS Publication #46, NTIS, April 1977.

[6] A. Baggio,"Wireless sensor networks in precision agriculture", in ACM Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Stockholm, Sweden, June 2005.

[7] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson,"Wireless Sensor Networks for Habitat Monitoring", in First ACM Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA, September 2002.

[8] G. Fuchs, S. Truchat, F. Dressler,"Distributed Software Management in Sensor Networks using Profiling Techniques", in 1st IEEE/ACM International Conference on Communication System Software and Middleware (IEEE COMSWARE 2006): 1st International Workshop on Software for Sensor Networks (SensorWare 2006), New Dehli, India, January 2006.

Miss D.Sunitha well known Author and excellent teacher Received B.Tech(CSE) and (M.Tech (CSE)) from NOVA College of Engg and Tech ,jangareddygudem,WG DT ,AP.Jawaharlal Nehru Technological University is working as Asst Professor in Computer Science and Engineering from Sree vani College of Engineering and Technology, He has 2 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences / journals . His area of Interest includes OperatingSystems,Database Management System,Compiler Design, mobile computing, computer organization and other advances in computer Applications.

Mr. Ch.Raja Jacob, well known Author and excellent teacher Received M.C.A and M.Tech (CSE) from Acharya Nagarjuna university is working as Associate Professor and HOD, Department of MCA, M.Tech Computer science engineering , Nova college of Engineering and Technology, He is an active member of ISTE.he has 7 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.