K.Britto Rosy, Dr.V.Palanisamy / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.

Implementation of Secure Reliable Communication Protocol in Mobile Ad hoc Networks

K.Britto Rosy[1], Dr.V.Palanisamy[2]
Department of Computer Sci and Engg
Alagappa University, Karaikudi. Tamilnadu India

Abstract

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. It is a collection of large number of mobile nodes that form temporary network. It completely different from other network. Due to the nature of MANETs, it more and more attacks from several sources. In this proposed work the SRCP (Secure Reliable Communication Protocol) for MANETs and a mobile agent system is a platform that can create, interpret, execute, transfer, and terminate mobile agents. A mobile agent system is regarded as an attractive technology when developing distributed applications. However, mobility makes it more difficult to trace agents. It is also more complex for agents to communicate with each other in a reliable manner. Therefore, a reliable communication protocol is necessary to control and monitor mobile agents and deliver messages between them. In this paper, a new Secure Reliable Communication Protocol (SRCP) is proposed for a multi region mobile agent computing environment. SRCP fulfills the following design goals: reliability, asynchrony, timeliness, location dependency, scalability, and communication cost.

Keywords: MANETs, Security, Mobile agents, communication, location management, message delivery, reliability.

1. INTRODUCTION

A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless links. *Ad hoc* is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet .Basic action of Ad hoc Networks useful when infrastructure not available, impractical, or expensive military applications,

rescue, home networking. MANET Also one of the ad hoc network used by some home network based working criteria. In MANET each nodes are connected via wireless link and free to move in communication with other [2]. The path between each pair of users may have multiple links, this allows an association with various link to be a part of same network. The network topology may change with time as the nodes move or adjust their transmission and reception parameters. And also it contain some basic limitations are packet loss due to transmission errors, variable capacity links and limited communication and bandwidth. It has extensive application, e.g. Personal area networking (cell phone, laptop, ear phone), Civilian environments (meeting rooms) etc.

There are large numbers of routing protocol have been proposed by researcher but no one can secure in all security aspects and also there is no security mechanism to detect malicious and selfish node collectively. The secure routing protocols are mainly divided into two categories: proactive protocols that maintain routes to all destinations whether it is needed or not, such as DSDV and reactive protocol that discover routes to its destination when it required, such as AODV. ASRP follows the reactive approach to sending the data or information to other nodes within the network [2]. Also we implement a mechanism, Extended Public key Cryptography (EPKCH) that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality and Non-Repudiation. In a mobile agent computing environment, a mobile agent must be able to communicate with other mobile agents or users in order to monitor their states, control them (for example, kill or suspend), interact with one other, or return results. However, the mobility of agents makes it more difficult to trace mobile agents and transfer messages reliably.

2. RELATED WORK

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad hoc mobile networks. Because of the difficulty of testing an ad hoc routing protocol in a real-world environment, a simulation was first created so that the protocol design could be tested in a variety of scenarios. Once simulation of the protocol was nearly complete, the simulation was used as the basis for an implementation in the Linux operating system. In the course of converting the simulation into an implementation, certain modifications were needed in AODV and the Linux kernel due to both simplifications made in the simulation of AODV and to incompatibilities of the Linux kernel and the IP-layer to routing in a mobile environment. This paper details many of the changes that were necessary during the development of the implementation.

A routing protocol that is appropriate for an ad hoc network is needed. But research into routing protocols for ad hoc networks so far have mainly targeted efficiency and assume a trusted environment. But these protocols are not

well operated in the networks that adversaries exist in. We propose a new on-demand secure routing protocol for ad hoc networks using an ID based cryptosystem. Our protocol can authenticate all nodes in the routing path with less network resource consumption than previous secure routing protocols. And our protocol does not need the fixed infrastructure without unrealistic assumptions because of using an ID based cryptosystem.

rotecting the network layer from malicious attacks is an important yet challenging security issue in mobile ad hoc networks. In this paper, we describe a unified network-layer security solution for such networks that protects both routing and data forwarding operations through the same reactive approach. SCAN does not apply any cryptographic primitives on the routing messages.

Instead, it protects the network by detecting and reacting to the malicious nodes. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. In essence, SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. Through both analysis and simulation results, we demonstrate the effectiveness of SCAN even in a highly mobile and hostile environment.

A mobile agent system is regarded as an attractive technology when developing distributed applications. However, mobility makes it more difficult to trace agents. It is also more complex for agents to communicate with each other in a reliable manner. Therefore, a reliable communication protocol is necessary to control and monitor mobile agents and deliver messages between them. In this paper, a new Reliable Communication Protocol (RCP) is proposed for a multi region mobile agent computing environment. RCP is implemented on the ODDUGI mobile agent system. Analysis and evaluation show that RCP fulfills the following design goals: reliability, asynchrony, timeliness, location dependency, scalability, and communication cost.

3. Working procedure in SRCP

In this work a reliable communication protocol that provides efficient location management and reliable message delivery is fundamental to the development of mobile agent systems. However, some problems remain unresolved. First, existing protocols apart from the SPC protocol do not consider multi region computing environments. Second, they do not guarantee the delivery of messages. In other words, a tracking problem occurs; a message follows a mobile agent without being delivered to the agent. A message is just sent to the nodes that the mobile agent left without delivery. Third, no protocols deal with location management and message delivery of cloned mobile agents and parent-child mobile agents. In a mobile agent computing environment, a mobile age NT can be cloned or a child mobile agent can also be created because a mobile agent is a software program. To solve the problems, a new Secure Reliable Communication Protocol (RCP) is proposed for multi region mobile agent computing environments. RCP tightly couples message.

3. Proposed Method:

Our proposed secure protocols aim to protect the network from attackers. Our proposed schemes work under several assumptions as follows:

Secure Reliable Communication Protocol algorithm

1. The network link is bidirectional. That is, if node A is able to transmit to node B, then B is also able to transmit to A. At a time the node can either malicious or selfish.

2. The wireless interface supports promiscuous mode operations. That is, each node can receive a copy of the messages being transmitted by other nodes within its receiving range.

3. A public key infrastructure exists in the MANET under consideration. Each mobile node stores the public key of all other nodes.

4. The trust relation could be instantiated. For example: by knowing public key of other nodes.

5. There is a security association between source node and destination node.

6.The existence of security association is justified because, host chose to employ a secure communication schemes and consequently, should be able to authenticate each other.

To solve the problems, a new Secure Reliable Communication Protocol (SRCP) is proposed for multiregional mobile agent computing environments. SRCP tightly couples message delivery with migration of mobile agents in order to deliver messages reliably and efficiently, thereby solving the tracking problem with low communication cost. In addition, it tackles communication of both cloned and parent-child mobile agents. It guarantees reliable delivery of messages. SRCP is implemented on the ODDUGI mobile agent system . Analysis and evaluation show that SRCP fulfills the following design goals: reliability, asynchrony, timeliness, location dependency, scalability, and communication cost.

3.1 Reliable communication protocol form Multi region mobile agents

The RCP for mobile agents is described considering a multi region mobile agent computing environment. RCP uses a region server that maintains location information of mobile agents within a region. It is also responsible for message delivery to all the mobile agents in its region by placing a blackboard. It tightly relates message delivery to migration of mobile agents. RCP consists of a Location Management Phase (LMP) and a

Message Delivery Phase (MDP). LMP is a procedure in which a mobile agent registers the location to its LS, its HN, or RSs when it is created or when it migrates. MDP is a procedure where in a sender delivers a message to a receiver agent while locating it. Fig. 3 shows the overall SRCP procedures and describes LMP and MDP in a multi region mobile agent computing environment. The LS maintains fAgentID; H N addrg entries; the field AgentID represents the identity or name of an agent; and HNaddrrepresents the address of an HN, where an agent is created first. The RS maintains fAgentI D; RN addr; NextRS addr; M sgsg entries; the field RNaddr represents the address of an RN, where a mobile agent resides and is to be found; Next RSaddr represents the address of the next RS to which a mobil e agent has migrated; and Msgs represents messages maintained in a blackboard. The HN maintains f AgentI D; RS addr g entries; RSaddr represents the address of the current RS in which a mobile agent resides and is to be found; Next RSaddr represents the address of the next RS to which a mobile agent has migrated; and Msgs represents messages maintained in a blackboard. The HN maintains f AgentI D; RS addr g entries; RSaddr represents the address of the current RS in which a mobile agent resides.

4. Experimental Results and Discussions:

The source (node 10) is broadcasting RREQ message to all its neighbors and Node 1which is the destination node, is sending RREP (route reply) back to the source. The nodes with the same frequency will receive the message and forward it to its neighbor, while the nodes with different frequency will drop the packet. In figure 4.2, a packet of blue color is on transmission from the source (node 10) to the destination (node 1). Since there is peer-to-peer communication between source node (10) and destination node (1), so no packet will be dropped.

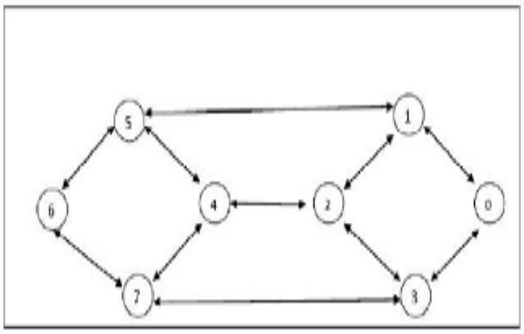

Fig 4. SIMULATED MANET

The simulation results are perform as follows

1. Network input by adding the node in form of adjacency list.

2. Simulate the packet transfer in the Initializing Mode.

3. Simulate the packet transfer in the Lazy Mode.

4. Simulate the packet transfer in the Packet Forwarding Mode Since the ASRP is a proactive secure routing protocol, so in every step it displays the status of tables of all the nodes.

The MDP uses a blackboard to deliver messages to a mobile agent, ensuring that a mobile agent in transit can receive messages reliably. Each RS stores and maintains messages on it s blackboard. The MDP follow s two approaches: reactive and proactive (see Fig. 5). The reactive approach delivers a message to a mobile agent when a mobile agent updates its location to the current RS (that is, when a mobile agent migrates). It is classified into four stages as follows:

1. A sender finds the HN's address of the receiver agent by contacting the LS, and then, the address of the current RS from the HN.

2. A sender sends the message to the RS.

3. The RS puts the message on its blackboard.

4. When the RS receives a location update message from the receiver agent, the RS checks its blackboard. If there is a message, the RS retrieves it from the blackboard, and then, delivers it to the receiver agent.

With the reactive approach, a mobile agent can check its messages on a blackboard upon migration. As a result, the reactive approach provides periodicity of message delivery and guarantees message delivery to mobile agents under migration.

5. CONCLUSION

In this paper Security is a significant issue in Mobile Ad hoc Networks. Intrusion of malicious nodes may cause serious impairment to the security. In the presented work, we have discussed all the modes of ASRP (simple mode and frequency hopping) along with their working and we proposed and implemented SRCP, a new communication protocol for mobile agents in a multi region mobile agent computing environment. SRCP decreases communication cost and offers reliability by solving the tracking problem with low communication cost and delivering a message to a mobile agent in transit. In addition, it deals with location management and message delivery of cloned mobile agents and parent-child mobile agents in the centralized and distributed approaches, thereby guaranteeing message delivery of these mobile agents. Analysis and evaluation shows that SRCP can achieve reliability, asynchrony, timeliness, location dependency, scalability, and low communication cost. We sincerely hope that our work will contribute in providing further research directions in the area of security based on frequency hopping. In this thesis work, ASRP over MANETs is simulated with different operation modes.

6. References:

[1] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.

[2] C.E. Perkins, P. Bhagwat, "Highly Dynamic Destination Sequenced Distance-vector Routing (DSDV) or Mobile Computers",Computer Communications Review, pp. 234-244, October, 1994.

[3] C. E. Perkin and E. M. Royer, " The Ad hoc On-Demand Distance Vector Routing Protocol," in C. E. Perkin (ed.), Ad hoc Networking, pp 173-219, Addison-2000

[4] B. Dahill, B. Levine, E. Royer, and C. Shields. A Secure Routing Protocol for Ad Hoc Networks. Technical Report UMCS- 2001-037, CS Dept., Umass 2001.

[5] H. Yang, X. Meng and S. Lu: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks, ACM, 2002.

[6] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Englewood Cliff, NJ 07632, 2002

[7] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Network," in Proc. CNDS 2002.

BIOGRAPHY

Ms.K.Britto Rosy

Ms.K.Britto Rosy is a Research scholar in the Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.C.A in Computer Science from Bishop Heber arts and science collage, Trichy, Tamilnadu in the year of 2011. She has presented her work in various national and international level conferences. Her areas of research interests include Network information security, Ad hoc wireless networks & security.

Dr. Palanisamy Vellaiyan

Dr. Palanisamy Vellaiyan obtained his B.Sc. degree in Mathematics from Bharathidasan University in 1987. He also received the M.C.A., and Ph.D Degrees from Alagappa University in 1990 and 2005 respectively. After that working as Lecturer in AVVM Sri Pushpam College, Poondi from 1990 to 1995, He joined Alagappa University as Lecturer in 1995. He is currently working as Associate Professor and Head of Department of Computer Science and Engineering. He also received the M.Tech., Degree from Bharathidasan University in 2009. He has published over 20 journals and conferences and his research interest includes Computer Networks & Security, Data Mining & Warehousing, Mobile Communication and computer algorithms.