DESIGN OF A SCHEME FOR SECURE ROUTING IN MOBILE AD HOC NETWORKS

V.Sesha Bhargavi[1] Dr.M.Seetha[2] Dr.S.Viswanadharaju[3]

[1]Assistant Professor, Department of Information Technology, GNITS, Hyderabad, India
b.velagaleti@gmail.com
[2]Professor, Department of Computer Science, GNITS, Hyderabad, India
smaddala2000@yahoo.com
[3]Professor, Department of Computer Science, SIT,JNTUH,Hyderabad, India
viswanadha_raju2004@yahoo.co.in

ABSTRACT

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wireline networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. So,we focus on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel.

KEYWORDS

Security, Ad hoc Network, Mobile Network ,mobile application

1. INTRODUCTION AND LITERATURE SURVEY

An ad hoc network is a set of wireless mobile nodes that form a dynamic autonomous network without the intervention of centralized access points or base stations. Unlike traditional wireless networks, ad hoc networks require no fixed network infrastructure and can be deployed as multihop packet networks rapidly and with relatively low expense. Such networks can be very useful in scenarios where natural conditions or time constraints make it impossible to pre-deploy infrastructure. Examples of applications include battlefields, emergency services, conference rooms, and home and office. Mobile nodes in an ad hoc network have limited radio transmission range. Nodes that are unable to communicate directly with each other require that intermediate nodes forward packets for them. Each node acts both as a router and as a host. The function of a routing protocol in ad hoc network is to establish routes between different nodes.

Natarajan Meghanathan, et al. (Eds): ITCS, SIP, JSE-2012, CS & IT 04, pp. 33–46, 2012.
 DOI : 10.5121/csit.2012.2104

Several ad hoc routing protocols have been proposed, which include AODV [1], [2], DSR [3], ZRP [4], TORA [5], DSDV [6],TBRPF [7], and others. Although they represent important steps in ad hoc routing research area, they still have security vulnerabilities, and can be attacked [8]. The special characteristics of ad hoc networks put forward challenges not present in traditional wired networks. In the traditional Internet, routers within the central parts of the network are owned by a few well known operators and are therefore assumed to be more trustworthy [9]. This assumption no longer holds in an ad hoc network since neither centrally administrated secure routers nor a strict security policy exists in an ad hoc network, and allnodes entering the network are expected to take part in routing. Also, because the links are usually wireless, any security that was gained because of the difficulty of tapping into a network is lost. Furthermore, because the topology in such a network can be highly dynamic, traditional routing protocols can no longer be used. Thus an ad hoc network has much higher security requirements than the traditional networks and the routing in ad hoc networks is hard to accomplish securely, robustly and efficiently.

The general purpose of securing ad hoc routing protocols is to protect the routing messages, to prevent attackers from modifying these messages or even injecting harmful routing messages into the network. So integrity and authenticity of routing messages should be guaranteed. Confidentiality can be ensured easily, e.g., by encryption, but it will increase overhead. Route establishment should be a fast process. If too much security mechanisms are built in, the efficiency of routing protocol may be sacrificed. So there is a tradeoff between security and efficiency.

In ad hoc network, the network topology is dynamic. Different packets exchanged between the same two nodes may go through different routes, among which there may be attackers lurking. Nevertheless, without online trusted servers as in wired networks, it is difficult to be acquainted with the trustworthiness of each node, thus keeping away malicious nodes from the routes.

2. RELATED WORK:

Yi et al. [12] developed a secure aware routing (SAR) protocol for ad hoc networks, which extended the Ad Hoc On-demand Distance Vector (AODV) routing protocol. In their protocol, the nodes in an ad hoc network have different security attributes and are classified into different trust levels. The trust level can be decided by an internal hierarchy of privileges in an organization. The nodes of the same trust level share a secret key. When a source constructs a route discovery message, it also specifies the required security level for the route. The route discovery message can also be encrypted by using the secret key shared by nodes of same trust level. Only the intermediate nodes that satisfy the required security level can process the message since only these nodes can decrypt the message. Other nodes just drop it. This protocol provides some protection to routing messages. The remaining problems are: Is the trust level fixed or can be changed? How to distribute key within the same trust level?

Papagiotis and Haas [13] proposed a secure routing protocol (SRP) for ad hoc networks. The assumption of SRP is the existence of a Security Association between a source node and a destination node, through which the source node and the destination node can authenticate each other. SRP is base on source routing. The source node broadcasts a route request to discover a route to the destination node. When an intermediate node receives the route request, it appends its identifier in the request packet and relays the request. So when the destination node receives the route request, a route has been set up and carried in the route request. The destination node generates a route reply containing the route and sends it back to the source node along the reverse of the route. The most important secure measure used in SRP is Message Authentication Code, which is calculated by using the shared secret key between the two ends. Both the unchanged

fields of route request and the route reply are covered by a MAC so that modification and IP spoofing from non-colluding attackers can be prevented during the process of route discovery.

Venkatraman and Agrawal [14] proposed a protocol based on public key cryptography. They assume the existence of a governing authority for the distribution of public keys. A source node generates a route request and digitally signs it using its private key. When a destination node sends a route reply back to the source node, public key cryptography is used for pair-wise authentication to exclude malicious nodes. If a node does not know a forwarding node's public key, they have to exchange public keys first. This pair-wise authentication is done by challenge and response process. The purpose of this protocol is to prevent external attacks.

A different approach, authenticated routing for adhoc networks (ARAN), was developed by Dahill et al. [15]. ARAN relies on public key cryptography for authentication. They assume that each node has a public/private key pair, and there exists a trusted certificate server to issue a certificate to each node. ARAN consists of two stages. The goal of stage one is for a source node to set up a route to a destination node. The source node broadcasts a route discovery packet, containing its certificate and digitally signed by using its private key. When a node receives the packet, it signs the packet using its private key and attaches to the packet its certificate and broadcasts the packet. Upon receiving the packet, a node verifies the signature with the attached certificate. The node then removes the signature of the broadcasting node, signs the packet with its private key, attaches its certificate, and rebroadcasts the packet. Eventually the destination node receives the packet and validates the signatures of the source node and the forwarding node with their certificates. The destination node constructs a reply, signs it and unicasts the reply back to the source over the reverse path. When an intermediate node receives the reply, with the same process as the route discovery packet, it verifies the signature, replaces the signature with its signature and relays the packet. Finally the source node can receive the reply. The optional second stage is used to discover the shortest path between two ends. The source node broadcasts a Shortest Path Confirmation message, which contains the same information as the route discovery packet plus the certificate of the destination node. The route discovery part of the Shortest Path Confirmation message is signed by the source and encrypted using the destination node's public key. When an intermediate node receives the message, it signs the message, appends its certificate, encrypts the message using the destination node's public key, and rebroadcasts it. When the destination node receives the message, it can know the length of the path from the included cryptographic credentials of the intermediate nodes.

Several protocols [16]–[19] based on public key cryptography have been proposed to protect routing protocols for wired network. Several efficient signature schemes based on hashing chains [20] have been proposed to protect routing messages [21]–[24] and broadcast message [25]–[27] of wired network.

Hu et al. [34], [35] and Zapata [28] adopted hashing chains to authenticate routing updates for ad hoc network situation. Perrig et al. [29] utilized hashing chain in securing sensor network.

Marti et al. [30] proposed a watchdog and pathrater scheme to improve the throughput of an ad hoc network in the presence of misbehaving node. Watchdog keeps track of misbehaving nodes. Pathrater avoids routing through those misbehaving nodes.

Yang et al. [31] extended AODV with a self-organized security approach. A token is utilized for authentication within the network, which is issued with a decentralized scheme [31]. Only with a valid token, can a node participate in route discovery and data packet delivery. Their protocol does not assume the existence of centralized trusted severs and is suitable for ad hoc network situation.

Awerbuch et al. [32] proposed a fault detection scheme to detect malicious links on a route between a source and a destination. The scheme is based on acknowledgements from some probe nodes on the route, which are specified by the source node. If the number of acknowledgement loss exceeds a particular threshold, a faulty link is considered to exist in the route. Then a binary search can detect the faulty link.

2.1 TYPES OF ROUTING PROTOCOLS:

There are several routing protocols proposed for wireless ad hoc networks. Classification of routing protocols is as given below:

- Proactive or table-driven routing protocols
- Reactive or on-demand routing protocols.
- Hybrid routing protocols.

Pro-active or Table-Driven routing protocols require each node to maintain up-to-date routing information to every other node (or nodes located within a specific region) in the network. On-demand routing protocols are designed to reduce the overheads in Table-Driven protocols by maintaining information for active routes only as and when required. Hybrid protocols combine the features of both proactive and reactive routing strategies to scale well with the increase in network size and node density. Following protocols are compared in this paper by evaluating the performance of each on the basis of PDR, end to end delay and throughput.

A. On Demand Multicast Routing Protocol (ODMRP):

ODMRP is a mesh based rather than conventional tree based scheme and uses a forwarding group concept [4]. The drawbacks in maintaining multicast trees in ad hoc network are frequent tree reconfiguration and non-shortest path in a shared tree. In ODMRP, group membership and multicast routes are established by the source on demand when a multicast source has packets to send, but no route to the multicast group, it broadcasts Join-Query control packets to the entire network. This control packet is periodically broadcast to refresh the membership information and updates routes.

B. Ad hoc On-demand Distance Vector Routing (AODV):

AODV is a reactive protocol in which the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up-to-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbours can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbours [10].

C. Fisheye State Routing (FSR) :

Application layer routing has received little attention in the ad hoc domain. An application layer approach has various advantages like routing is easy to deploy. It does not require changes at the

network layer. The construction of logical structure hides routing complications such as link failure instances, which are left to be taken care of at routing layer. Application layer routing exploits the capabilities of lower layer protocols in providing reliability, congestion control, flow control or security according to the needs of application.

The Fisheye State Routing (FSR) algorithm for ad hoc networks introduces the notion of multi-level "scope" to reduce routing update overhead in large networks. A node stores the link state for every destination in the network. It periodically broadcasts the link state update of a destination to its neighbours with a frequency that depends on the hop distance to that destination (i.e., the "scope" relative to that destination)[11]. FSR is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbours and the detail and accuracy of information decreases as the distance from node increases.

2.2 PROBLEMS WITH THE EXISTING PROTOCOLS:

A) ***On Demand Multicast Routing Protocol (ODMRP):***

1. No explicit leave message (member nodes refreshed when needed by source)
2. Multiple path to one destination (mesh approach)
3. Backup path if link is broken (Robust)
4. High Overhead (because broadcast the reply to many nodes)
5. Complex Topology

B) Ad hoc On-demand Distance Vector Routing (AODV):

The disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route Reply packets in response to a single RouteRequest packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption. Longer delay and greater packet loss when unsuccessful.

C) ***Fisheye State Routing (FSR) :***

It is easy to locate destinations due to the flat addressing scheme and topology map, but this also limits scalability. Other negative points are the routing table storage complexity and the processing overhead. FSR doesn't provide any form of security, as most other protocols.

2.3 PROPOSED WORK

Problems with Location-Based Mobile Applications

Integrating location information into an application may possibly be the most exiting possibility for mobile applications [Michael Juntao Yuan]. Location information offers a whole new realm of applications. The biggest single problem with location information is not in the technology, but in the use of it: privacy. Whereas knowing the location of the mobile user can be very handy in offering very useful services, it can also violate basic privacy rights of a user. So, the users are often faced with a choice whether to "opt-in" or "opt-out"; participating in the program means signing a form that basically gives up a great deal of privacy, but not signing results in a lack of

access to the desired services. Currently, there are no technologies that allow for "opting-in" or "opting-out" of sharing ones location on a granular interactive basis. In other words, there is no easy way for the user to specify when, where and how his or her location should be known and when, where and how his or her location should not be known. The second and third biggest problems with today's location systems are price and power use. Good GPS-based systems are still fairly expensive and if we want to add GIS information to that to get value-added services such as finding restaurants etc. we are looking at subscription fees. Also, most location devices are considerable drain on the batteries, though this is an area of focus in the location industry and should be addressed with in the near future.

Security and Privacy of Mobile Location Information:

Security and Privacy are of utmost importance to location-based services. Without providing proper security and privacy, few users are willing to use a system that can reveal their current location or history of locations to third parties. Examples of problems that may arise if proper security is not implemented for location services are unwanted marketing, invasion of privacy by governmental or commercial entities, and identity theft or other criminal activities [Patrick Stuedi]. There are several aspects to security and privacy of location information, the most important are the following:

1. Access Security: There must be a proper authentication and authorization mechanism in place for those systems that access the location of a given device. Any systems that can obtain location information must in turn provide secure access to any related data through proper authentication and authorization.
2. Data Security: Any system used to cross-reference any information that identifies the user associated with a device through profiles; billing etc. must be completely secured. The content that specifies the location of the device must be transmitted through a secure mechanism (e.g. encryption)
3. User Control: The user must have control in specifying whether the location of his or her device is shared with any secondary systems within or outside of the primary wireless network.

Some of the key features of a system that offers location-based service and the clients to such a system must be the following:

1. The system must allow the users to configure policies regarding where and when their location information may be obtained and/or shared.
2. The system must allow the users to specify with whom their location information may be shared.
3. The system must automatically remove all historical data about a user's location unless otherwise allowed by the user.
4. The location-based service must not expose specific information to its client systems on why the location of a particular user may not be available. For example, the client system must not be able to request whether the user has specified to be unavailable to that particular client or during a particular time window.
5. The error margin in the exact location of the user must not be provided unless specified by the user.
6. The client system must specify a reason for which the location is obtained. Only trusted systems should be able to obtain location information.

2.3.1 Mobile XML and Web Services

XML (eXtensible Markup Language) has already become the de facto standard for exchange of human-readable data. Whether such will be the case for machine-to-machine communication is questionable; nevertheless, such applications exist and their popularity is increasing. A variety of XML-based technologies for Mobile applications have been evolved. RDF (Resource Description Framework), a part of the Semantic Web that is becoming pervasively more crucial to mobile applications. CC/PP Composite Capabilities / Preference Profiles and UAProf (User Agent Profile) are applications of RDF and XML for mobile applications, and even XML can be mapped to UML. (Unified Modeling Language) at the architectural level. The significance of XML to mobile applications is twofold. First, it offers well-formed and deterministically modifiable format for human-readable data, and second, it offers interoperability. Building mobile applications now always uses XML as one of the core pieces in their infrastructure.

2.3.2 Cell phone Security

One of the most widely deployed cellular networks is the Global System for Mobile Communications (GSM). The designers of GSM or 2G (second-generation cellular networks) had several goals in mind. Better quality for voice, higher speeds for data, and other non-voice application and international roaming were some of the goals. From a security viewpoint, it was also designed to protect against charge fraud and eavesdropping.

The successor to GSM is Universal Mobile Telecommunications Systems (UMTS) or simple 3G. It promised advanced services such as Mobile Internet, multimedia messaging, videoconferencing, etc. UMTS standards were defined by an international consortium/standardization organization called 3GPP (Third generation Partnership Research implementation). The security provided in GSM is a quantum leap over that provided in first generation cellular networks. Still, there are several lacunae in 2G that have been plugged in 3G networks.

3. IMPLEMENTATIONS AND VALIDATIONS

3.1 Case 1. Safe Passwords in mobile phone

Safe passwords in mobile phone: These days, anyone who is on the web needs too many passwords, and it's impossible to remember them all. Generally if we have too many passwords to remember we will be writing them all down on a piece of research implementation and hide it somewhere. We designed password safe application as another solution. It's a small program that encrypts all of your passwords using one paraphrase. The program is very easy to use, and isn't bogged down by unnecessary features. This application provides security through simplicity.
This is an end–user java application that stores sensitive information like passwords on mobile phones with strong encryption. This uses **SHA encryption technique** to secure the information. The application requires Java Micro Edition (J2ME) with MIDP-1.0, which is available on most current phones. Modules involved: Security Module, Password Storage Module, and Password Retrieval Module.

Security Module: In this module we use the SHA algorithm to encrypt and decrypt the password which is required to enter into the application.

Password Storage Module: In this module the user can store his passwords into the application.

Password Retrieval Module: In this module user can view his passwords by login in to the application.

The Figure1 consists of sequence diagram of the safe passwords in mobile phone application.

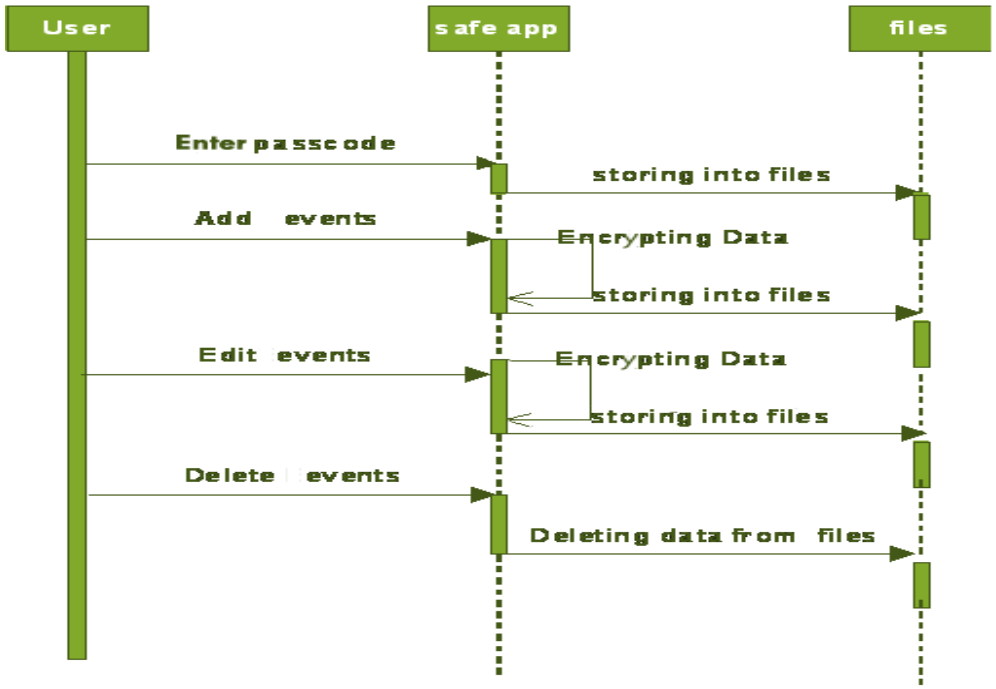
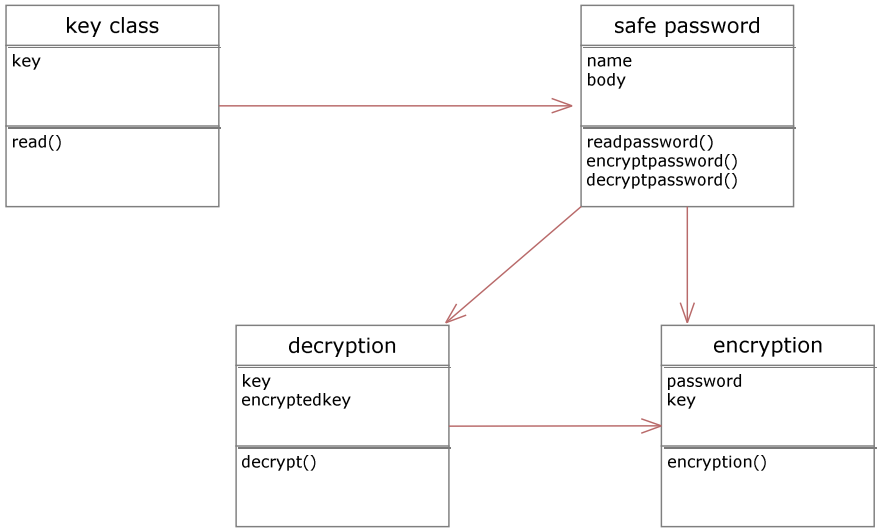


Figure1 Sequence diagram of the safe passwords in mobile phone



The Figure2 consists of the class diagram of the safe passwords in mobile phone application.

Figure 3 consists of the execution screen shot of the proposed implemented application

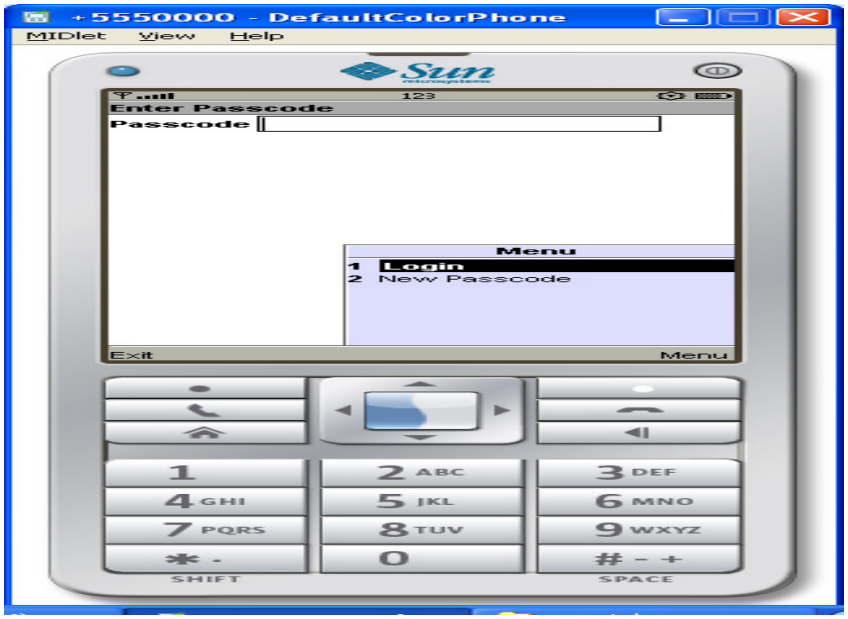


Figure 3 Execution Screen shot of the Mobile phone application

3.2 Case2. Spatial Mobile Privacy Web Service Application

This case study discusses about privacy issues and implementations of Spatial Web Services Security Architectures. Role-Based Access Control (RBAC) Model is a widely deployed model in commercial systems and for which a standard has been developed. The widespread deployment of location-based services and mobile applications, as well as the increased concern for the management and sharing of geographical information in strategic applications like environmental protection and homeland security has resulted in a strong demand for spatially aware access control systems. These application domains impose interesting requirements on access control systems. In particular, the permissions assigned to users depend on their position in a reference space; users often belong to well-defined categories; objects to which permissions must be granted are located in that space; and access control policies must grant permissions based on locations and user positions. In this implementation, we want to review various strategies for Geo-RBAC and its future research work for grid computing, virtualized environments and cloud Spatial computing.

In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it also raises concerns over potential intrusion into user location privacy. To protect location privacy, one typical approach is to cloak user locations into spatial regions based on user-specified privacy requirements, and to transform location-based queries into region-based queries. We study the representation of cloaking regions and show that a circular region generally leads to a small result size for region based queries. Moreover, the progressive query processing mode achieves a shorter response time than the bulk mode by parallelizing the query evaluation and result transmission.

The Disruptive Cloud Cloud computing is a service consumption and delivery model that can help improving business performance, control costs and ultimately transform business models.

Cloud computing can bring opportunities to many, ranging from businesses that consume IT infrastructure, to providers of such infrastructure, general users and government as well [Hiren Bhatt].

The Figures. 4, 5, 6 below provides the class diagram, sequence diagram, and execution screen shot respectively of the spatial mobile privacy web service application

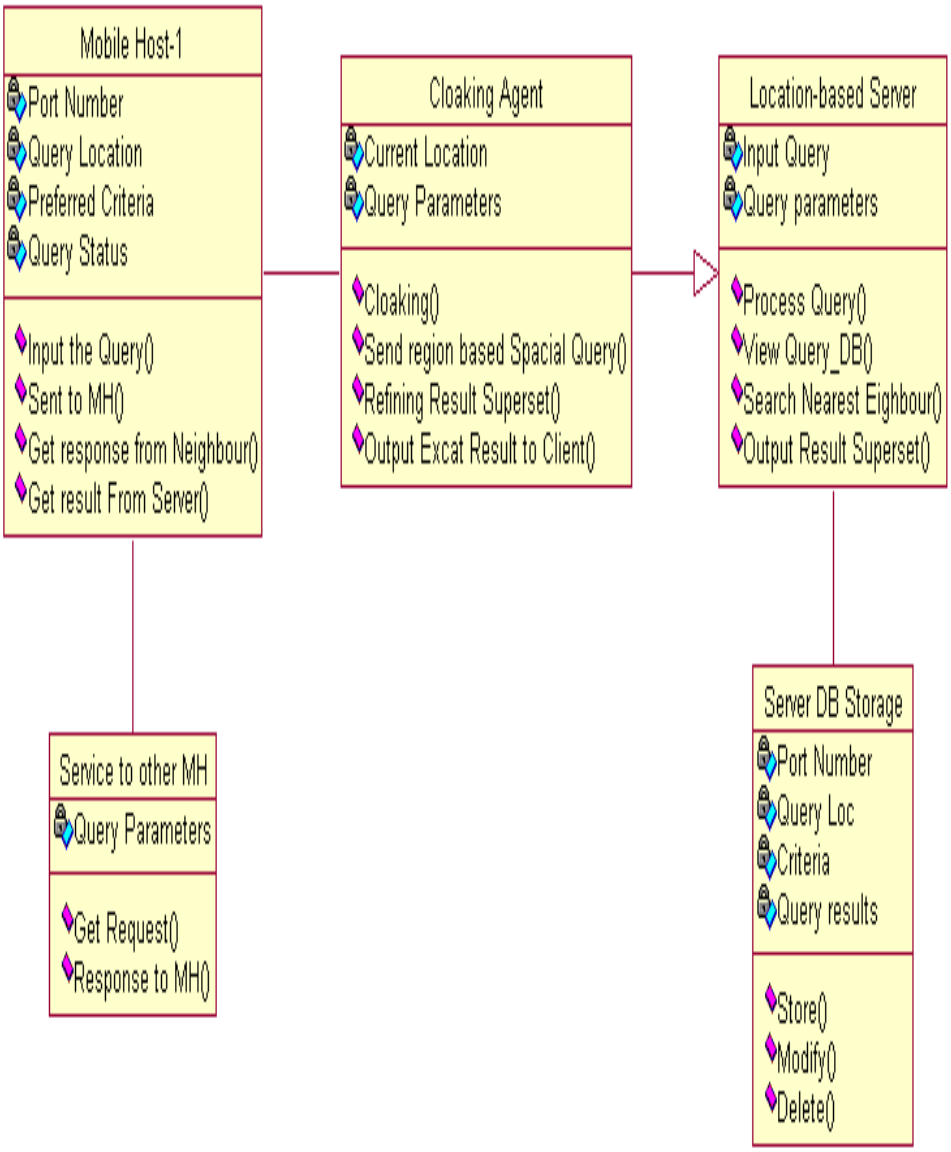


Figure 4 Class diagram of spatial mobile privacy web service application

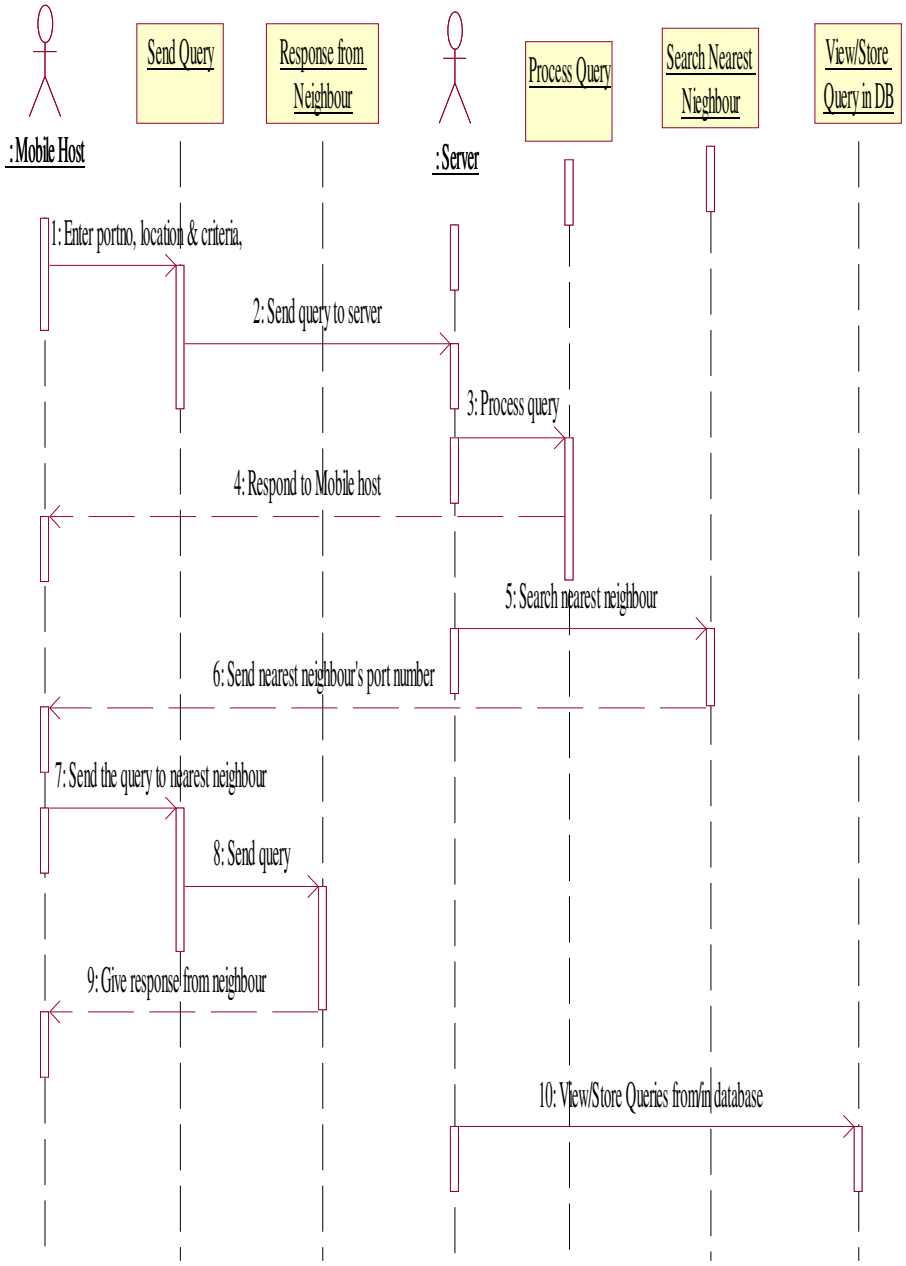


Figure 5 Sequence diagram of spatial mobile privacy web service application

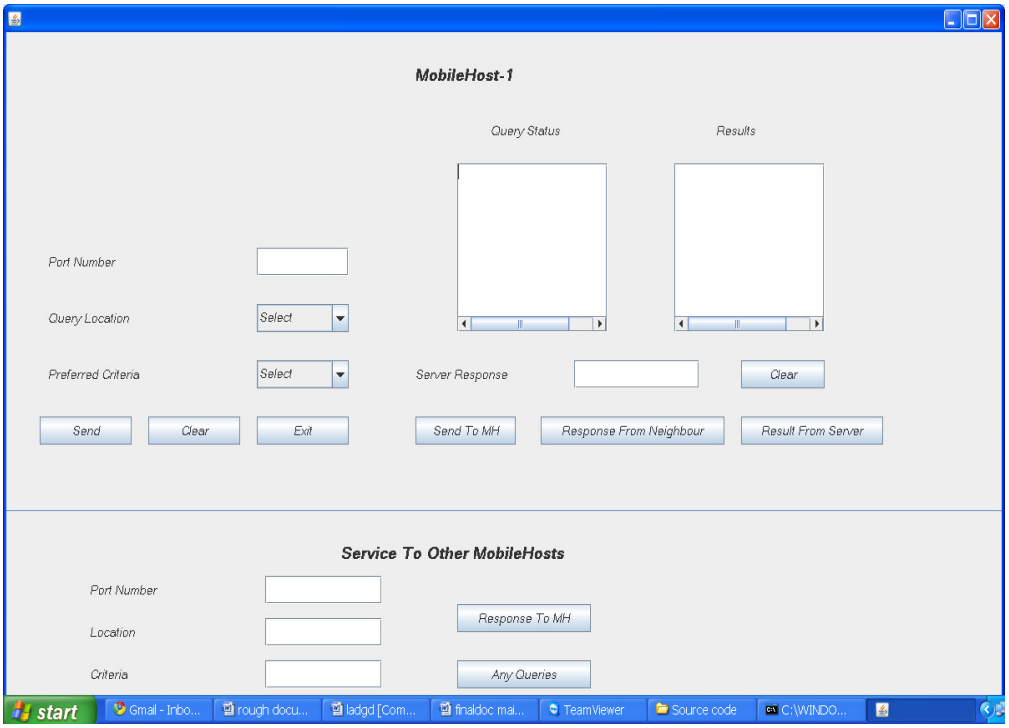


Figure 6 Execution screen shot of spatial mobile privacy web service application

4. CONCLUSIONS

AODV does not specify any special security measures. The proposed protocol, CAODV would be considered as an endeavor to enhance the security requirements of AODV operated MANETs. In the proposed protocol authentication is achieved by double encryption of session key using asymmetric cryptography (using public and private keys of source and destination respectively). Data confidentiality and integrity can be achieved by data encryption using strong symmetric key algorithm such as AES. Thus the proposed protocol which is implemented in a single step will inherent added advantages over other security conscious protocols designed for AODV.

REFERENCES

[1] C. E. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999, pp. 90–100.

[2] E. Royer and C. Toh, “A review of current routing protocols for ad-hoc mobile wireless networks,” IEEE Personal Communications, April 1999.

[3] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” Mobile Computing, vol. 353, pp. 153–181, 1996.

[4] Z. J. Haas, “A new routing protocol for the reconfigurable wireless network,” in Proceeding of 1997 IEEE 6th International Conference on Universal Personal Communications Record: Bridging the Way to the 21st Century (ICUPC’97), October 1997, pp. 562–566.

[5] V. Park and M. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in Proc. of INFOCOM'97, 1997.

[6] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in Proceedings of the ACM SIGCOMM'94. ACM Press, 1994, pp. 234–244.

[7] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-path Forwarding (TBRPF)," Request for Comments RFC 3684, February, 2004, February 2004

[8] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, November/December 1999.

[9] S. Wu, F. Wang, and B. Vetter, "Secure routing protocols: Theory and practice," NC State Univ., Tech. Rep., April 1998.

[10] A Secure Routing Protocol for Wireless Ad Hoc Networks Huaizhi Li Department of Computer Science University of Kentucky Lexington, KY 40506 Email: hli3@cs.uky.edu Mukesh singhal Department of Computer Science University of Kentucky Lexington, KY 40506

[11] Addressing Security Concerns of Data Exchange in AODV Protocol Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam World Academy of Science, Engineering and Technology

[12] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks, Tech. Rep. UIUCDCS-R-2001-2241, August 2001.

[13] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[14] L. Venkatraman and D. P. Agrawal, "Security scheme for routing in adhoc networks," in Proceedings of the 13th International Conference on Wireless Communications, July 2001, pp. 129–146.

[15] B. Dahill, B. Levine, C. Shields, and E. Royer, "Secure routing protocol for ad hoc networks," U Mass, Tech. Rep. UM-CS-2001-037, 2001.

[16] B. Smith and J. Garcia-Luna-Aceves, "Securing the border gateway routing protocol," in Proceedings of Global Internet, November 1996.

[17] B. Smith, S. Murthy, and J. Garcia-Luna-Aceves, "Securing distancevector routing protocols," in Proceedings of the Symposium on Network and Distributed System Security (SNDSS'97), February 1997, pp. 85–92.

[18] S. Murphy and M. Badger, "Digital signature protection of the OSPF routing protocol," in Proceedings of the Symposium on Network and Distributed System Security (SNDSS'96), February 1996, pp. 93–102.

[19] R. Perlman, "Network layer protocols with byzantine robustness," PhD thesis, MIT LCS TR-429, October 1988.

[20] R. C. Merkle, "A digital signature based on a conventional encryption function," in Advances in Cryptology-CRYPTO'87, August 1987.

[21] S. Cheung, "An efficient message authentication scheme for link state routing," in 13th Annual Computer Security Applications Conference, 1997.

[22] R. Hauser, T. Przygienda, and G. Tsudik, "Reducing the cost of security in link-state routing," in Symposium on Network and Distributed System Security (SNDSS'97), February 1997, pp. 93–99.

[23] L. Reyzin and N. Reyzin, "Better than BiBa: Short one-time signatures with fast signing and verifying," in Information Security and Privacy-7th Australasian Conference ACSIP, 2002.

[24] K. Zhang, "Efficient protocols for signing routing messages," in Proceedings of the 1998 Internet Society (ISOC) Symposium on Network and Distributed System Security, March 1998.

[25] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in 8th ACM Conference on Computer and Communication Security, November 2001.

[26] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient and secure source authentication for multicast," in Network and Distributed System Security Symposium, NDSS'01, February 2001.

[27] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient authentication and signing of multicast streams over lossy channels," in IEEE Symposium on Security and Privacy, May 2000.

[28] M. G. Zapata, "Securing ad hoc routing protocols," in Workshop on Wireless Security (WiSe'02), September 2002.

[29] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of MOBICOM, 2001.

[30] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proceedings of MOBICOM 2000, August 2000.

[31] H. Yang, X. Meng, and S. Lu, "Self-organized network layer security in mobile ad hoc networks," in Workshop on Wireless Security (WiSe'02), September 2002.

[32] H. Luo and S. Lu, "Ubiquitous and robust authentication services for ad hoc wireless networks," UCLA Computer Science, Tech. Rep. 200030, October 2000.

[33] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An ondemand secure routing protocol resilent to byzantine failures," in Workshop on Wireless Security (WiSe'02), September 2002.

[34] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in 4th IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[35] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in 8th ACM International Conference on Mobile Computing and Networking (MobiCom 2002), sssSeptember 2002.