ISSN 2278-8808 SJIF 2014 = 4.889
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

RESOLVING PROTECTION AND AUTHENTICATION ISSUES OF PERVASIVE COMPUTING EVNIRONMNET IN EPIDEMIC CONDITIONS

Mr. Gurav Yogesh Bhaskarrao

Abstract

Context administration in pervasive/epid environments must reflect the particular qualities of these environments, e.g. dispersion, mobility, asset obliged devices, or heterogeneity of context sources. Despite the fact that various context models have been displayed in the writing, none of them backings these necessities to a sufficient degree in the meantime. In this work, we exhibit a complete furthermore incorporated methodology for context modeling in pervasive computing environments . The proposed scheme flawlessly integrates two underlying cryptographic primitives, blind mark and hash chain, into a profoundly adaptable and lightweight authentication what's more key station protocol. The scheme gives express common authentication between a user and a service while permitting the user to namelessly cooperate with the service. Separated service access control is additionally empowered in the proposed scheme by arranging mobile users into diverse service bunches. In this work, we examined security issues and their current results in the mobile ad hoc network. This study depicts the crucial problems of ad hoc networking by providing for its related exploration foundation including the idea, gimmicks, status, and requisitions of MANET. Neighborhood Discovery (ND), namely, the discovery of devices directly reachable for communication or in physical proximity, becomes a fundamental requirement and a building block for various applications.

1. INTRODUCTION

Pervasive computing in wireless environment is a rapidly developing area of Information and Communications Technology (ICT). The term refers to the increasing integration of ICT into people's lives and environments, made possible by the growing availability of microprocessors with inbuilt communications facilities. These devices will range from a few millimeters in size (small sensors) to several meters (displays and surfaces). They may be interconnected via wired and wireless technologies into broader, more capable, networks. The model includes a highly dynamic load-time system supporting application discovery, resource and capability negotiation, and application apportioning.

The run-time system allows the resources to be dynamically shared among client devices and servers. It also includes monitoring and check pointing, and enables a running application to migrate from device to device or to simultaneously utilize the interface capabilities of

multiple devices. Mobile Ad hoc NET works (MANETs) have attracted great research interest in recent years. A mobile ad hoc network is a self-organizing multi-hop wireless network where all hosts (often called nodes) participate in the routing and data forwarding process. The deployment of ad hoc networks does not rely on fixed infrastructures such as router and base station, thereby posing a critical requirement on the nodes to cooperate with each other for successful data transmission. Many works [01], [05] have pointed out that the impact of malicious and selfish users must be carefully investigated. Existing cooperation enforcement techniques cannot be adapted for some of recent advance in routing protocols. In particular, we are going to study in the new Connectionless-Oriented Approach. There are 2 such techniques, namely Connectionless Approach(CLA) and Contention-Based Forwarding(CBF).

These techniques do not maintain a hop-by-hop route for a communication session to minimize the occurrence of broken link. In CLA, the network area is divided into non-overlapping grid cells, each serving as a virtual router . Any physical router (i.e., mobile host), currently inside a virtual router, can help forward the data packet to the next virtual router along the virtual link. This process is repeated until the packet reaches its final destination. Since a virtual link is based on virtual routers which do not move, it is much more robust than physical link. Another scheme, CBF, simply forwards data packets to the next hop without first having to establish the one-hop connection. The nodes that happen to be in the general direction towards the destination node help to forward the data packets.

As pervasive devices get fused in our day-to-day lives, security will progressively turning into a typical sympathy toward all users however for most it will be a bit of hindsight, in the same way as other computing capacities. The ease of use and development of pervasive computing provisions depends extraordinarily on the security and unwavering quality gave by the requisitions. One of the real tests wireless sensor networks confront today is security. While the sending of sensor nodes in an unattended environment makes the networks powerless against a mixture of potential assaults, the natural force and memory impediments of sensor nodes makes expected security results unfeasible. However, the very nature of wireless mobile networks makes it easy to abuse ND and thereby compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and to secure ND is crucial. In this article, we focus on this problem and provide definitions of neighborhood types and ND protocol properties, as well as a broad classification of attacks. Our ND literature survey reveals that securing ND is indeed a difficult and largely open

problem. Moreover, given the severity of the problem, we advocate the need to formally model neighborhood and to analyze ND schemes.

Execution degradation because of routing overhead is a genuine obstruction to satisfying quality of service (QoS) in mobile ad hoc networks (Mantes). Accordingly, dissecting the effect of routing overhead in an ongoing environment gets basic to creating effective routing protocols and provisioning network execution. We create a factual systematic methodology to contemplating the effect of the routing overhead on postponement and throughput in a constant MANET test bed. Many pervasive devices can discretionarily join and leave a network, making a nomadic environment known as a pervasive ad hoc network. Privacy and security are two critical however apparently contradictory goals in a pervasive nature's domain (PCE).Owe to the powerless nature of the mobile ad hoc network, there are various security threats that aggravate the advancement of it. We first analyze the fundamental vulnerabilities in the mobile ad hoc networks, which have made it much less demanding to experience the ill effects of assaults than the traditional wired network.

The objective of this research is to address the cooperation issue for connectionless-oriented approach in wireless ad hoc networks. There can be both selfish and malicious nodes in a mobile ad hoc network. The selfish nodes are most concerned about their energy consumption and intentionally drop packets to save power. The purpose of malicious node is to attack network using various intrusive techniques. In general, nodes in an ad hoc network can exhibit Byzantine behaviors. That is, they can drop, modify, or misroute data packets. As a result, the availability and robustness of the networks are severely compromised. Many works and have been published to combat such problem misbehaving nodes are detected and a routing algorithm is employed to avoid and penalize misbehaving nodes. These techniques, however, cannot be applied to the connectionless-oriented approach since any node in the general direction towards the destination node can potentially help forward the data packets.

2. LITERATURE REVIVES

Wireless computing technologies

Wireless computing involves three converging areas of ICT: computing (‘devices’), communications (‘connectivity’) and ‘user interfaces’.

Devices

PCS devices are likely to assume many different forms and sizes, from handheld units (similar to mobile phones) to near-invisible devices set into ‘everyday’ objects (like furniture and clothing). These will all be able to communicate with each other and act ‘intelligently’.

Such devices can be separated into three categories:

- Sensors: input devices that detect environmental changes, user behaviors, human commands etc;
- Processors: electronic systems that interpret and analyze input-data.
- Actuators: output devices that respond to processed information by altering the environment via electronic or mechanical means. For example, air temperature control is often done with actuators.

However the term can also refer to devices which deliver information, rather than altering the environment physically. If the current wireless and Mobile Adhoc Network (MANET) routing topology is unknown and there are no long-term node identities and no option to check how do nodes communicate? One possibility is to use a *hit-and-miss* approach, which we adopt in a thesis[1] . In it, a node picks a geographical location (coordinates), draws a certain perimeter around it (e.g., by specifying a radius or points of a polygon) uses the resulting area as the destination address. The message (route request) addressed in such a way propagates through the network (via flooding, as in AODV) and either fails to find any nodes in the specified area or reaches one or more. Destination node(s) then reply (if they want to) using state along the reverse route, with intermediate nodes using information cached during route request processing.

This simple location-based technique is effective as it guarantees that, as long as the network is connected, all destinations within the specified area are reached. However, it complicates operation since the specified area might be empty. In this case, the source needs to either expand the perimeter or try a different area altogether.[1].The most relevant body of wireless and MANET research tackles secure anonymous reactive MANET routing, e.g., SPAAR [2], AO2P [3], ASR [4], MASK [5], ANODR [6], D-ANODR [7], ARM [8], ASRP [9] and ODAR [10]. A survey comparing ANODR, ASR and discussing general anonymity and security issues in wireless and MANET routing protocols can be found in [27]. Of the anonymous reactive protocols, SPAAR [1] and AO2P [2] require on-line location servers. ASR [3] and ARM [8] assume that each authorized source-destination pair pre-shares a unique secret key. An on DSR [11], ASRP [12], EARP [13] and ARMR [14] assume that each source destination pair shares some secret information, which could be the public key of the destination or a secret key.

ANODR [6] assumes that the source shares some secret with the destination for the construction of a trapdoor, for example the destination's TESLA [15] secret key. SDAR [16]

assumes that the source knows the public key of the destination, obtained from a certification authority (CA), and ODAR [10] requires an on-line public key distribution server. MASK [5] and DANODR [7] contain the final destination in the clear in each RREQ message. AMRSS [17] and ARMR [14] utilize multiple paths for routing. AMRSS [17] assumes that the entire network shares a pair of public private keys and that the destination ID will be encrypted under the public key. AMRSS also includes the entire path encrypted under the network key in each data message.

In addition, all aforementioned protocols assume that nodes know long-term identities of all other nodes, i.e..the communication paradigm is identity-centric.

Research Methodology

Study of existing issues in pervasive computing including security and privacy issues

- Detailed analysis of pervasive computing and different MANET routing protocols
- Data collection and testing by Simulation using tools like NS2 for analysis.
- Testing of research goals with results and parameters.
- Conceptual frame work design for provisions in pervasive computing.

3. EXISTING SYSTEM

Nowadays, when we need to gain access to the WWW (World Wide Web), we end up remaining in front of Personal computers which are aggregations of a NC (Network Computer), and which are sending and getting such a large amount of data. These devices constrain the client to have least specialized learning to gain access to the internet to utilize new media including Web destinations, streaming sound and feature, talk rooms, email, online groups, Web advertising, DVD and CD-ROM media, virtual actuality situations, and so on.

There are numerous types of devices other than computers associated with the Web, Laptops, telephones, printers, robot arms, cameras, pagers, Handheld devices (PDA (personal digital associate), mobiles, and so forth). The flighty development of wireless access to the Internet provides for you the chance to check your email and most loved Web destinations while you're on the path to your employment or to anyplace as well. The customers utilize these devices (wireless, PDA) with advanced innovations, to check their E-mail. Also the engineers are experiencing this pattern by making Web destinations that are modified for handheld devices that hold. These incorporate everything on the internet that convey news headlines, stock quotes, and other often redesigned information, to shopping destinations.

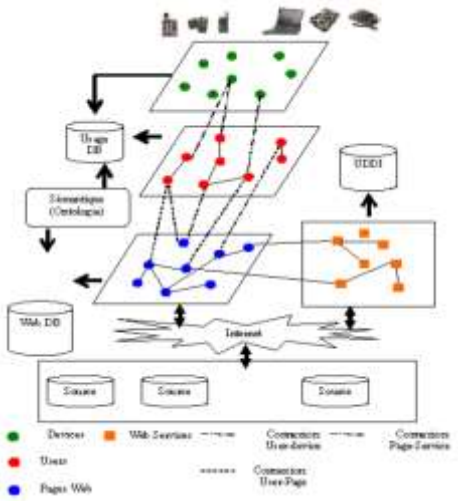

Fig 1: System Architecture

4. PROPOSED SYSTEM

The final implementation of pervasive environment involves the use of devices by average users and not only by researchers. The implementation of security schemes need to be transparent to the end user. A number of security technologies are already available on almost all layers of protocol stacks. The implementation and configuration of these schemes are already complex and the involvement of end user to configure and implement these schemes will make the pervasive environment vulnerable to a lot of security loop holes. A weak link in the environment might give a trust level to malicious user who can further use the resources as authorized user. Therefore, security schemes must be user friendly for deployment of security and building of trust.

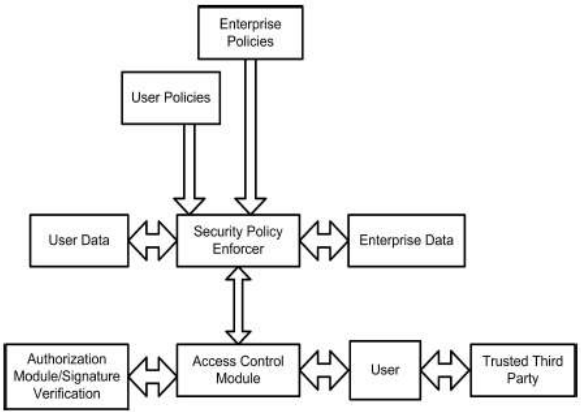

Fig: 2: Proposed Systems

The arrangement of sensor nodes in an unattended environment makes the networks helpless. Wireless sensor networks are progressively being utilized within military, natural, health and business provisions. Sensor networks are intrinsically unique in relation to traditional wired

networks and wireless ad-hoc networks. Security is an critical characteristic for the sending of Wireless Sensor Networks. This study outlines the ambushes and their orders in wireless sensor networks and likewise an endeavor has been made to investigate the security component widely used to handle those assaults. In this part we have depicted the four primary parts of wireless sensor network security: deterrents, prerequisites, assaults, and protections. Firstly, the foundation information of MANET are presented MANET idea, characteristics, current status, and provision areas. Different intriguing issues are explored that blanket all parts of ad hoc wireless networks. In the mean time, numerous routing protocols intended for ad hoc networks have been proposed as Internet Draft and RFC of IETF. MANETs might be abused in a wide area of provisions, from military, crisis salvage, law requirement, business, to local and personal connections. The security of WSNS has turned into a major subject subsequent to of the diverse dangers showing up and the hugeness of data classifiedness, despite the fact that in the past, there was a little focus on WSNS security. Mobile ad hoc networking is a standout amongst the most significant and vital advances that help future pervasive computing situation. The unique characters of MANET bring this innovation extraordinary chances together with serious challenges. Presently MANET is getting to be more fascinating examination subject and there are numerous exploration ventures utilized by academic and organizations everywhere throughout the world. Different intriguing issues are researched that blanket all parts of ad hoc wireless networks. Then, numerous routing protocols intended for ad hoc networks have been proposed as Internet Draft and RFC of IETF. Mantes. MANETs can be exploited in a wide area of applications, from military, emergency rescue, law enforcement, commercial, to local and personal contexts. Finally, this thesis presents the testing of our proposed algorithms and protocol sachems in a simulated environment .NS2 is a fundamental tool for testing adhoc and wireless network in a virtual environment ,in general where wireless networks that require verifying distances between and/or locations of groups of nodes. It is particularly important in location-based MANET store prevent location-fraud attacks. that protocols and mechanisms developed in this thesis address important security and privacy issues fundamental to eventual adoption of location-based MANETs.

5. FUTURE SCOPE

The way mobile computing devices and applications are developed, deployed and used today does not meet the expectations of the user community and falls far short of the potential security for pervasive computing. The proposed model can be implemented in real life

applications to improve privacy and security in ubiquitous environment.

6. CONCLUSION

Pervasive computing research field is still in its infancy and a lot of research efforts needs to be done to see the actual implementation of real pervasive environment. A lot of focus is being given on the service discovery, context acquisition, context categorization and context modeling in context aware computing. Web services are used for integrating information sources from both inside and outside an enterprise.Web services are simpler, standards-based, and more loosely coupled technology for connecting data, systems, and organizations. Although security schemes are derived to be implemented in the pervasive environment but they are being implemented into already existing pervasive computing architectures. No generalized architecture exists in pervasive environment therefore schemes are implemented differently in each case. The study presents a web services architecture for implementing security in pervasive environment using standard based technologies which are widely used and implemented.

Finally, this work presents the testing of our proposed algorithms and protocol sachems in a simulated environment .NS2 is a fundamental tool for testing adhoc and wireless network in a virtual environment ,in general where wireless networks that require verifying distances between and/orlocations of groups of nodes. It is particularly important in location-based MANETsto prevent location-fraud attacks. We believe that protocols and mechanisms developed in this work address important security and privacy issues fundamental to eventual adoption of location-based MANETs.

REFERENCES

Karim El Defrawy, Gene Tsudik, Privacy-Preserving Location-Based On-Demand Routing in MANETs ,IEEE JOURNAL ON SELECTED AREAS IN COMMUNI ,CATIONS, VOL. 29, NO. 10, DEC, 2011

S. Carter and A. Yasinsac, "Secure position aided ad hoc routing," Proc. IASTED International Conference on Communications and Computer Networks (CCN02), pp. 329–334, 2002.

X. Wu and B. Bhargava, "Ao2p: ad hoc on-demand position-based private routing protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335–348, July-Aug. 2005.

B. Zhu, Z. Wan, M. Kankanhalli, F. Bao, and R. Deng, "Anonymous secure routing in mobile ad-hoc networks," Local Computer Networks, 2004. 29th Annual IEEE International Conference on, pp. 102–108, Nov. 2004.

Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: anonymous on-demand routing in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 5, no. 9, pp. 2376–2385, September 2006.

J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in ACM MobiHoc '03.New York, NY, USA: ACM, Jun ,2011, pp. 291–302.

L. Yang, M. Jakobsson, and S.Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," Securecomm and Workshops, 2006, pp. 1–10, 28 2006-Sept. 1 2006.8

S. Seys and B. Preneel, "Arm: anonymous routing protocol for mobile ad hoc networks," Int. J. Wire. Mob. Comput., vol. 3, no. 3, pp. 145–155, 2009.

Y. Cheng and D. Agrawal, "Distributed anonymous secure routing protocol in wireless mobile ad hoc networks," OPNETWORK, 2005.

D. Sy, R. Chen, and L. Bao, "Odar: On-demand anonymous routing in ad hoc networks," Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on, pp. 267–276, Oct. 2006.

E. Kumari and A. Kannammal, "Privacy and security on anonymous routing protocols in manet," in Computer and Electrical Engineering, 2009. ICCEE '09. Second International Conference on, vol. 2, 28-30 2009, pp. 431–435.

R. Song, L. Korba, and G. Yee, "Anondsr: efficient anonymous dynamic source routing for mobile ad-hoc networks," in SASN '05. NewYork, NY, USA: ACM, 2005, pp. 33–42.

S. Chen and M. Wu, "Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks," in Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on, vol. 1, 13-14 , Oct 2011, pp. 582–585.

Y. Dong, T. W. Chim, V. O. K. Li, S. M. Yiu, and C. K. Hui, "Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1536–1550, 2009.

A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol," RSA CryptoBytes, vol. 5, p. 2002, 2002.

A. Boukerche and K. E.-K. et al., "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks," Elsevier Computer Communications, 2005.

H. L. J. M. Xiaoqing Li and W. Zhang, "An efficient anonymous routing protocol for mobile ad hoc networks," in IAS, 2012, pp. 287–29