Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.94 – 96

RESEARCH ARTICLE

A Secure Protocol for Spontaneous Wireless Ad Hoc Network Creation

L.Dhanam[1], M.S Vinu[2]

[1]M.E Computer Science and Engineering,
Sri Eshwar College of Engineering, Anna University, India
[2]Professor, Department of CSE,
Sri Eshwar College of Engineering, Coimbatore, India

Abstract—

A secure protocol for spontaneous wireless ad hoc networks that uses an hybrid even or asymmetric and therefore the trust between users so as to exchange the data and exchange the key keys that may be used to write the data. Within the planned system, if a replacement node would like to with the prevailing node, the new node will send the request to the prevailing node. Supported the request, this node will send its public key to the new node. At that point the new node and existing node will share their public and private key components to authenticate each other. For security purpose the info are encrypted throughout transmission. The Certificate Authority is used to authorize the node once it wishes joins another node. Secret is generated, that's used to share the info and it'll be changed at a particular quantity of some time. Among the modification technique, the key secret is additionally changed once the node joins a network and leaves a network. Therefore we tend to are ready to increase the number of security.

Keywords— Distributed protocol, secure protocol, spontaneous network, wireless ad hoc networks

I. INTRODUCTION

Computer security is data security as applied to laptops and computer networks .The field covers all the processes and mechanisms by that computer-based instrumentation, data and services are protected against unmotivated or unauthorized access, modification or destruction. The term laptop security has evolved in recent years. Before the problem of information security became wide advertised within the media, most people's plan of computer security targeted on the physical machine.

A spontaneous network is a special case of ad hoc networks. They sometimes have very little or no dependence on a centralized administration. Spontaneous networks will be wired or wireless. We tend to consider solely wireless spontaneous networks. Their objective is the integration of services and devices within the same setting, enabling the user to own instant

service without any external infrastructure. As a result of these networks is enforced in devices like laptops, PDAs or mobile phones, with restricted capacities, they have to use a light-weight protocol, and new ways to manage and integrate them.

Configuration services in spontaneous networks rely considerably on network size, the character of the participating nodes and running applications. Spontaneous networks imitate human relations whereas having ability to new conditions and fault tolerance ways based on imitating the behaviour of human relations facilitate secure integration of services in spontaneous networks. Moreover, cooperation among the nodes and quality of service for all shared network services should be provided.

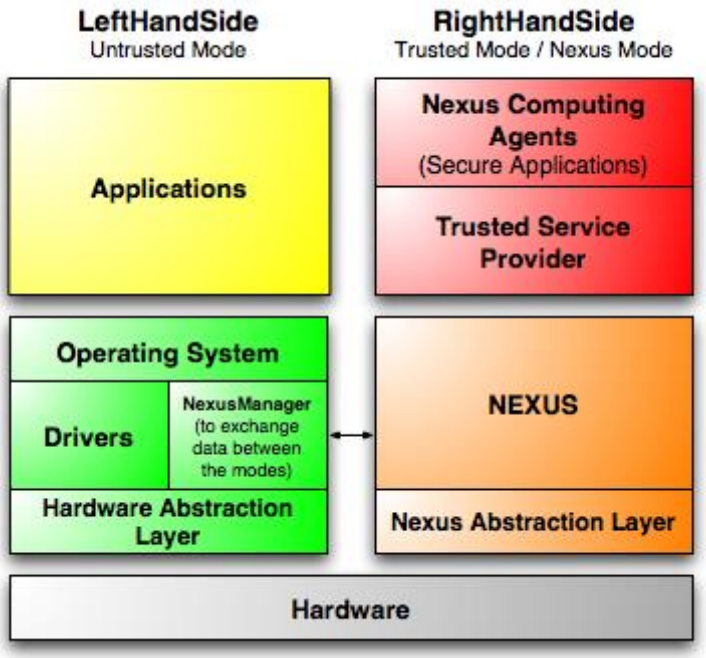

Figure 1.1 Architecture of secure computing

II. EXISTING SYSTEM

If there is no correct security measures were enforced in wireless ad hoc networks whereas new nodes and exchanging knowledge. A spontaneous network could be a special case of ad hoc networks. They typically have very little or no dependence on a centralized administration .dynamic networks with versatile memberships, cluster signature and distributed signatures are difficult to manage the scalability and adaptability of mobile communications increase users' productivity and efficiency.

Spontaneous ad hoc networks are formed by a group of mobile terminals placed during a close location that communicate with one another, sharing resources, services or computing time throughout a restricted amount of your time and during a restricted house, following human interaction pattern. Individuals are connected to a group of individuals for a while, and then leave. Network management should be clear to the user.

III. PROPOSED SOLUTION

In the system we have a tendency to propose, if a new node need to with the existing node, the new node can send the request to the existing node. Supported the request, the existing node can send its public key to the new node. And existing node can share their public and

personal key parts to manifest one another. For security purpose the information are going to be encrypted throughout transmission. The Certificate Authority is employed to authorize the node once it needs joins another node. Secret key is generated, that is employed to share the information and it will be modified at a specific amount of your time.

IV. CONCLUSION

We show the design of a protocol that permits the creation and management of a spontaneous wireless ad hoc network. It's supported a social network imitating the behaviour of human relationships. Thus, every user can work to maintain the network, improve the services offered, and supply data to alternative network users. A unique scientific discipline address is appointed to every device, the DNS is managed with efficiency and therefore the services can be discovered mechanically. We have also created a easy application that has stripped interaction with the user. A user without advanced technical data will started and participates during a spontaneous network. The safety schemes enclosed within the protocol enable secure communication between end users.

REFERENCES

[1] L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001.
[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.
[3] S. Preuß and C.H. Cap, "Overview of Spontaneous Networking - Evolving Concepts and Technologies," Rostocker Informatik- Berichte, vol. 24, pp. 113-123, 2000.
[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.
[6] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks with Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.
[7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hopby- Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
[8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
[9] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
[10] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications,vol. 12, no. 2, pp. 37-43, Dec. 2010.

AUTHORS BIOGRAPGHY

L.DHANAM received her B.E(CSE) Degree from Hindusthan college of Engineering and Technology,Coimbatore, Tamilnadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest is Network security, Operating system and Theory of Computation.

M.S.VINU has obtained her Post Graduate degree, M.E.(Computer Science and Engineering) in Nandha College of Engineering, Erode and obtained her Graduate degree B.E.,(Computer Science and Engineering) from VSB College of Engineering, Karur. She is currently serving as Assistant Professor of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu with a teaching experience of 2 years. She is specializing in the area of Network Security. India). Her area is Network Security and Wireless Sensor Network.

