International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 3, Issue 2 | ISSN 2321-6905 February-2015

International Journal of Science Engineering and Advance Technology

Procedure To Establish A Secure Self-Configured Environment For Data Distribution And Services Sharing Among Users

1**Syam Kumar Nallamothu**2**Amanatulla Mohammad,** 3**Sayeed Yasin**
Dept. of CSE, Nimra Institute of Science & Technology, Vijayawada, AP, India

Abstract:
A spontaneous network is a particular case of ad hocnetworks. They usually have little or no dependence on acentralized administration. Spontaneous networks can bewired or wireless. We regard as only wireless spontaneousnetworks in this paper. Their objective is the integration of services and devices in the same environment enabling theuser to have instant service without any external infrastructure.Because these networks are implemented indevices such as laptops, PDAs or mobile phones withlimited capacities they must use a lightweight protocol andnew methods to control manage and integrate them. To resolve mentioned securityissues we used an authentication phase and a trust phase. Moreover we presented a method to allow nodesto check the legitimacy of their IP addresses while notgenerating duplicated IP addresses. The mechanism helpsnodes to authenticate by using their IP addresses. We haveused this mechanism in the secure protocol presented inthis paper.

Keywords: Distributed protocol, secure protocol, spontaneous network, wireless ad hoc networks.

Introduction:
Spontaneous ad hoc networks necessitate well defined,efficient and user-friendly security mechanisms. Tasks to beperformed include user identification, their authorization,address assignment, name service, operation and safety.Usually wireless networks with infrastructure use CertificateAuthority (CA) servers to supervise node authenticationand trust. This paper presents a secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/asymmetric scheme and the trust between users in order to switch over the initial data and to replace the secret keys that will be usedto encrypt the data. Trust is based on the first visual contact between users. Our proposal is aabsolute self-configured secure protocolthat is able to create the network and share secure services without any infrastructure. The network allows sharing resources andoffering new services among users in a secure environment. The protocol includes all functions needed to operate without any externalsupport. We have designed and developed it in devices with limited resources. Network creation stages are detailed and thecommunication, protocol messages, and network management are explained. Our proposal has been executed in order to test theprotocol procedure and performance. Ultimately we compare the protocol with other spontaneous ad hoc network protocols in order toemphasize its features and we provide a security analysis of the system.

Relate Work: Gallo et al. pursued two targets in unpromptednetworks to make best use of responsiveness given some constraintson the energy cost and to minimize the energy costgiven certain requirements on the responsiveness. Liu et al. show how networked nodes can originallysupport and cooperate with each other in a peer-topeer(P2P) manner to quickly discover and self-configureany services available on the disaster area and bring areal-time capability by self-organizing themselves in spontaneousgroups to offer higher flexibility and adaptabilityfor disaster monitoring and relief.

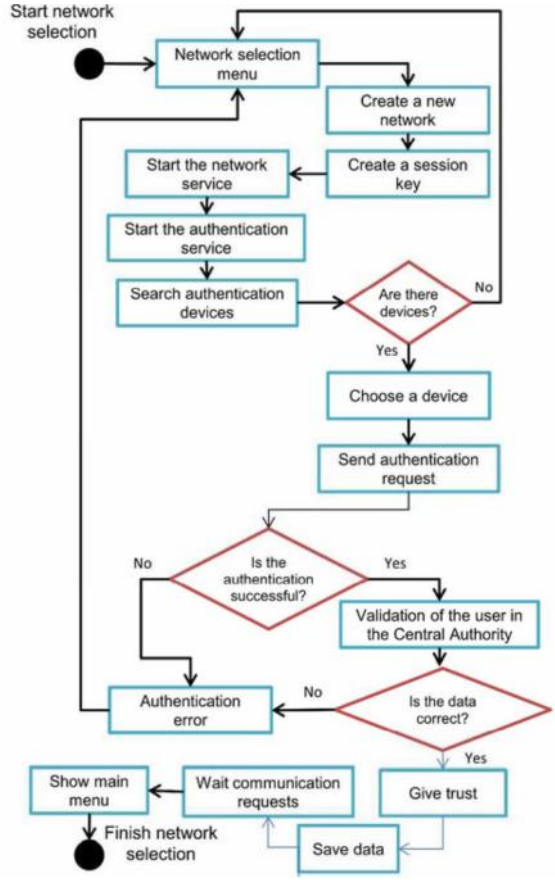
Existing Method:
The related literature shows quite a few security methodssuch as predistribution key algorithms symmetric andasymmetric algorithms, intermediate node-based methodsand hybrid methods. But these methods are notenough for spontaneous networks because they need aninitial configuration i.e., network configuration or externalauthorities.

Disadvantages:
None of the existing methods propose a secure spontaneousnetwork protocol based on user trust that providesnode authenticity, integrity checking, and privacy.

Proposed Method:
Security isestablished based on the service required by the users bybuilding a trust network to obtain a distributed certificationauthority. A user is able to join the network because he/sheknows someone that belongs to it. Thus, the certificationauthority is distributed between the users that trust the newuser. The network management is also distributed, whichallows the network to have a distributed name service.

Advantages:
Thenetwork and protocol proposed can establish asecure self-configured environment for data distributionand resources and services sharing among users.

Procedure For Network Creation:



Joining Procedure:

The system is based on the use of an Identity Card (IDC) anda certificate. The IDC contains public and private components.The public component contains a Logical Identity(LID), which is unique for each user and allows nodes toidentify it. It may include information such as name,photograph or other type of user identification. This ideahas been used in other systems such as in vehicular ad hocnetworks.

Services Discovery:

Auser can ask other devices in order to know the availableservices. It has an agreement to allow access to its servicesand to access the services offered by other nodes. Serviceshave a large number of parameters which are nottransparent to the user and require manual configuration.One issue is to manage the automatic integration tasks anduse, for example, service agents. Other is to manage secureaccess to the services offered by the nodes in the network.

Trusted Chain And Changing Trust Level:

The network is created using the information providedby users, thus, each node is identified by an IP address.Services are shared using TCP connections. Nodes can also send requests to update networkinformation. The reply will contain the identity cards ofall nodes in the network. The node replying to this requestmust sign this data ensuring the authenticity of theshipment. If it is a trusted node, its validity is also ensured,since trusted nodes have been responsible for validatingtheir previous certificates.

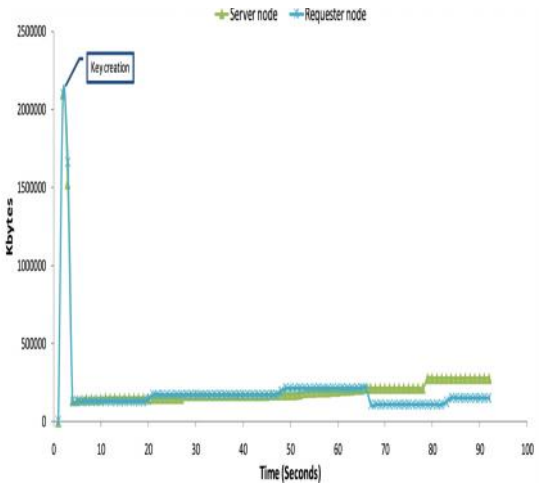
Protocol Operation:

The UML is avisual specification standardized language that is built tomodel object oriented systems. We use keys, activities, anduse cases (diagrams offered by the standard) to define theprocesses, the structure of the classes in the system, and thebehaviour of objects or operations.Once the validation/registration process of the user inthe device has been done, he/she must determine whetherto create a new network or participate in an existing one. Ifhe/she decides to create a new network, To request a certificate, the node sends a requestcertificate message to its trusted nodes. The applicationgenerates a packet to request the certificate to its trust nodeswhich are selected from the database.

Protocol Implementation:

When a device wants to join a spontaneous network ithas to start the process by sending a Discovery requestpacket which contains the Logical Identity of the userin order to let the destinations know the sender device. The receivers will reply with the Discovery reply packetwith their Logical Identity, their IP address, and networkmask. This information is then used to learn the selecteddevice to authenticate and to propose an IP inside thatnetwork IP range. The authentication request packet isused for the new device authentication. The authenticationreply packet confirms that the proposed IP and the emailare unique in the network, so the new device isofficially authenticated.

Experimental Results:



It shows when a new node joins thespontaneous network, by both nodes for all the processesfrom certificate creation to data transfer. The node thatgenerates the network uses more memory

because it is incharge of sending two messages for the authenticationprocess, one with the symmetric encryption and anotherwith asymmetric encryption.

Conclusion:

The design of the protocol is based on a social network imitating thebehaviour of human relationships that allowsthe creation and management of a spontaneous wirelessad hoc network. Each user will workto maintain the network, improve the services offered, andprovide information to other network users. the DNS can bemanaged efficiently and the services can be discoveredautomatically. We have also created a user-friendly applicationthat has minimal interaction with the user. A userwithout advanced technical knowledge can set up andparticipate in a spontaneous network. The security schemesincluded in the protocol allow secure communicationbetween end users.

References:

[1] L.M. Feeney, B. Ahlgren, and A. Westerlund, "SpontaneousNetworking: An Application-Oriented Approach to Ad-hocNetworking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181,June 2001.

[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented andService-Oriented Spontaneous Ad Hoc and Sensor WirelessNetworks," 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," RostockerInformatik-Berichte, vol. 24, pp. 113-123, 2000.

[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A SpontaneousAd-Hoc Network to Share WWW Access," EURASIP J. WirelessComm. and Networking, vol. 2010, article 18, 2010.

[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "ASurvey 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 Networkswith 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 HocNetworks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystemwithout 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 Schemewith Node Revocation for Wireless Sensor Networks," Ad Hoc andSensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

[10] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad HocNetwork (MANETs): Technical Review," Int'l J. Computer Applications,vol. 12, no. 2, pp. 37-43, Dec. 2010.

[11] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of SecurityAttacks on a New Security Protocol for Mobile Ad Hoc Networks,"Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.

[12] L. Herrero and R. Lacuesta, "A Security Architecture Proposal forSpontaneous Networks," Proc. Int'l Conf. Advances in the InternetProcessing System and Interdisciplinary Research, Oct. 2003.

Syam Kumar Nallamothu K.L.C.E(KoneruLakshmaiahCollegeofEngineering)Vaddeswaram,affiliatedUniversity:NagarjunaUniversity.MYM.TechProjet:ASecure Protocol for Spontaneous Wireless Ad Hoc Networks Creation.

AMANATULLAMOHAMD received his M.Tech from CSE-NIMRA college of Engineering & Technology (JNTUK, Kakinada), Ibrahimpatnam, Vijayawada. He is currently working as an Assistant Professor in NIMRA Institute of Science & Technology in the Department of Computer Science & Technology in the Department of Computer Science & Engineering, Ibrahimpatnam, Vijayawada. He has more than four years Experience in teaching. EMail:amanatulla@gmail.com

SAYEED YASIN received his MTECH in Computer Science &Engg from JNTU Hyderabad.He is pursuing Ph.D in Rayalaseema University ,Kurnool.He is currently working as Assoc. Professor & HOD in Nimra Institute of Science & Technology the Department of Computers Science and Engineering,Vijayawada.He has more than Eight years of experience in teaching.His area of interests are wireless networks & programming. E-Mail: sdyasin761@gmail.com